BJA
Bureau of Justice Assistance
U.S. Department of Justice

Face Recognition

Policy Development Template

For Use in Criminal Intelligence and Investigative Activities

December 2017

Where to Locate This Resource

This resource is available at www.it.ojp.gov and www.ncirc.gov. To request printed copies, send requests to information@ncirc.gov.

To Request a Word Version of the Template

To request a Word version, send requests to information@ncirc.gov.

Updates

This resource is considered a living document. Submission of feedback and content suggestions for periodic updates are encouraged and may be provided by e-mail to information@ncirc.gov.

This project was supported by Grant Number 2013-D6-BX-K001 awarded by the Bureau of Justice Assistance, in collaboration with the U.S. Department of Homeland Security. The Bureau of Justice Assistance is a component of the Department of Justice's Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, the Office for Victims of Crime, and the Office of Sex Offender Sentencing, Monitoring, Apprehending, Registering, and Tracking. Points of view or opinions in this document are those of the author and do not necessarily represent the official position or policies of the U.S. Department of Justice or the U.S. Department of Homeland Security.

Face Recognition Policy Template for State, Local, and Tribal Criminal Intelligence and Investigative Activities

(This Page Intentionally Left Blank)

Table of Contents

I. Introduction 1

A. Face Recognition Overview 3

1. How Do Face Recognition Systems Work? 3
2. Are Face Recognition Results Considered an Identification? 4
3. Is Face Recognition Information Considered Criminal Intelligence? 4

B. How to Use This Resource 4

1. Program Versus System 5
2. What Entities Should Use the Policy Template? 5
3. Transparency and Referencing Other Policies 6
4. Mobile Face Recognition Use 6
5. Face Recognition Analysis on Live Video 7
6. Template Modifications—Customizing Your Policy 7

C. Resource List 7

1. Face Recognition and Biometric-Related Resources 7
2. Policy Development Templates 9
3. Privacy Regulations and Authorities 10
4. Additional Privacy and Security-Related Resources 10

D. Acknowledgements 11

II. Face Recognition Policy Development Template for State, Local, and Tribal Criminal Intelligence and Investigative Activities 13

A. Purpose Statement 13

B. Policy Applicability and Legal Compliance 15

C. Governance and Oversight 16

D. Definitions 18

E. Acquiring and Receiving Face Recognition Information 18

F. Use of Face Recognition Information 20

G. Sharing and Disseminating Face Recognition Information 24

H. Data Quality Assurance 25

I. Disclosure Requests 26

J. Redress 26

J.1 Complaints 26

J.2 Requests for Corrections 27

J.3 Appeals 27

K. Security and Maintenance 27

L. Information Retention and Purging 31

M. Accountability and Enforcement 33

M.1 Transparency 33

M.2 Accountability 34

M.3 Enforcement 35

N. Training 35

Appendix A—Glossary of Terms and Definitions 39

Appendix B—Fair Information Practice Principles (FIPPs) 49

Appendix C—Listing of Federal Laws 53

Appendix D—Sample Face Recognition Policy 59

I. Introduction

Face recognition technology can be a valuable investigative tool to detect and prevent criminal activity; reduce an imminent threat to health or safety; protect the public; help identify persons unable to identify themselves, or deceased persons; and improve security and officer safety. The National Center for Missing and Exploited Children (NCMEC), for example, is using face recognition software to search the internet for these children. In the past, determining someone's identity was a manual drawn-out process of viewing mug shot images. The use of face recognition software is helping to streamline this process by returning investigative results quicker. The purpose of face recognition technology is not a new one, it's simply enabling law enforcement entities to complete an existing process more efficiently.

However, law enforcement's use of face recognition tools in investigative and criminal intelligence activities has been the subject of much scrutiny regarding concerns about the accuracy of the technology, use at First Amendment-protected events, and assertions that face recognition systems are being used without appropriate safeguards, such as law, policy, training, and audits. Since images of individual persons are the source of face recognition information, there are higher expectations for the protection of privacy, civil rights, and civil liberties (P/CRCL). Currently, there is no uniform set of rules in the United States governing the gathering, collection, use, sharing, and dissemination of information available through face recognition tools. The potential for misuse of face recognition information may expose agencies participating in such systems to civil liability and negative public perceptions. The lack of rules and protocols also raises concerns that law enforcement agencies will use face recognition systems to systematically, and without human intervention, identify members of the public and monitor individuals' actions and movements. Strong control and oversight of face recognition use are critical considerations in policy development and program implementation. Such efforts not only enhance mission effectiveness but also safeguard P/CRCL of individuals.

This policy development template was developed by state, local, and federal law enforcement, privacy, and criminal justice partners to provide law enforcement, fusion centers, and other public safety agencies with a framework for developing face recognition policies that comply with applicable laws, reduce privacy risks, implement minimum required training for authorized users and examiners, and establish entity accountability and oversight. In addition, this template includes policy provisions on collection, access, use, dissemination, data quality, security, redress, retention and purging, and accountability and enforcement, with an overall focus on ensuring the integration of P/CRCL protections in face recognition processes. Established Fair Information

Practice Principles form the core of the privacy framework for this template (see Appendix B). Note: The term "entity" is used throughout this resource to refer to the policy-authoring organization.[1]

When an entity determines to develop and implement a face recognition policy, it is important to note that crafting such a policy is not a one-time project; it is just one stage in an ongoing entity privacy program cycle:[2]

Stage 1. Educate and raise awareness on the importance of having P/CRCL protections.
Stage 2. Assess entity P/CRCL risks by evaluating the process through which the entity collects, receives, accesses, uses, disseminates, retains, and purges face recognition information.
Stage 3. **Develop a face recognition policy** to articulate the legal framework and policy position on how the entity handles face recognition.
Stage 4. Perform a policy evaluation and engage with community stakeholders, prior to publishing, to determine whether the policy adequately addresses current standards, P/CRCL protections, and the law.
Stage 5. Implement and train personnel and authorized users on the established rules and procedures.
Stage 6. Perform an annual policy review and make appropriate changes in response to implementation experience, guidance from oversight or advisory bodies, applicable laws, technology, and public expectations.
Stage 7. Audit the processes described in the face recognition policy.

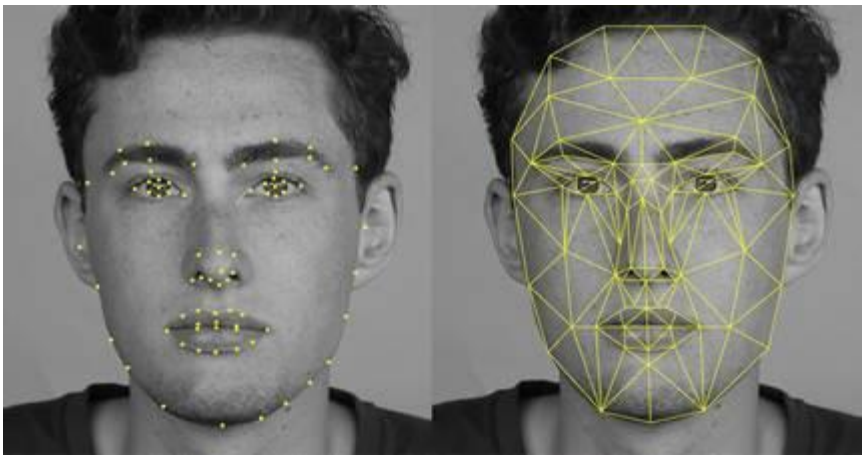
The implementation of proven policies and practices can mitigate the risk of negative impacts while improving mission effectiveness. As face recognition use expands, it is necessary for law enforcement, fusion centers, and other public safety agencies to ensure that comprehensive policies are developed, adopted, and implemented in order to guide the entity and its personnel in the day-to-day access and use of face recognition technology. Policies that are developed in a transparent manner and which are properly enforced foster trust—not only within and between justice partners but also by the public. This process helps ensure that justice entities are serving as responsible stewards of face recognition information and operating with respect for individual P/CRCL and the law.

BIOMETRICS POLICIES

This template was developed to address the use of face recognition technology by state, local, tribal, and territorial (SLTT) law enforcement and public safety entities and fusion centers through the development of P/CRCL policies. It was not, however, designed to cover all possible biometric modalities, such as fingerprints, palm prints, DNA, familial DNA searching, iris recognition, retina scan, voiceprint, etc. Specific and comprehensive policies are recommended that will appropriately address the use of each biometric technology, unique capture methods, complex processes and procedures, and P/CRCL protections.

[1] The term "entity" is used throughout this resource to identify the policy-authoring organization and differentiate it from external or participating agencies. Refer to the terms "agency," "entity," and "participating agency" in Appendix A—Glossary of Terms and Definitions for more information.
[2] Global Justice Information Sharing Initiative Privacy Resources, Bureau of Justice Assistance, Office of Justice Program, U.S. Department of Justice, https://it.ojp.gov/privacy.

A. Face Recognition Overview



Considering the potential benefits to public safety that face recognition technology can offer, it is important that law enforcement and public safety agencies establish the appropriate framework for ensuring that the technology will be used in a responsible manner that does not violate P/CRCL.

Use of face recognition technology is often misunderstood. It is not being used as an all-knowing big brother that keeps track of an individual's weekly—or daily—trips to a business. More accurately, it is a lead generator for law enforcement to investigate criminal activity, akin to a more reliable eye witness. Moreover, facial recognition is not a machine-dominated technology. Generally, entities use—and it is a good practice to do so—a two-part machine-human process—facial recognition, which is software based, and facial comparison, which is human based.[3]

1. How Do Face Recognition Systems Work?

During enrollment, an image (e.g., a photograph, a digital capture, or a video still) of a face of the known individual (such as a mug shot) is submitted to the face recognition system. While each system's techniques may vary, in general, the distinctive characteristics of each face, such as the distance between the eyes, the width of the nose, and the depth of the eye sockets, are measured. These characteristics are known as "nodal points." Nodal points are extracted from the face image and are transformed through the use of algorithms into a unique file called a "biometric template."[4] A biometric template is a reduced set of data that, in face recognition systems, represents the unique features of the enrolled person's face.

Biometric templates are then stored in a repository for future comparison with probe images of unknown persons, such as images gathered during a criminal investigation. During a face recognition search, the system compares the biometric template created from a probe (unknown) image with all of the face templates (of known persons) stored in the repository. The system then provides a list of the most likely candidate photographs (sometimes referred to as a "gallery"[5]). At this point in the process, the face recognition system has not made a formal identification.

Algorithms

Algorithms are mathematical equations—calculations, data processing, or automated reasoning—that are widely used throughout information technology and are the biggest factors in face recognition accuracy. Since the development of, and improvements in, algorithm performance are ongoing and ever evolving, they are not discussed in depth within this resource. However, policy provisions on data quality are provided in section H. Data Quality in the P/CRCL template contained in Chapter II. Entities are strongly encouraged to consider algorithm performance prior to purchasing a face recognition system.

Refer to the National Institute of Standards and Technology's (NIST's) Face Recognition Vendor Tests (FRVT), which provide independent government evaluations of commercially available and prototype face recognition technologies, https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt.

[3] Ibid.

[4] The term "template," in this usage (e.g., biometric template), is not to be confused with the term used in the title of this document, which means a template, or guide, for developing a face recognition policy. To avoid confusion, the term biometric template is not used in the rest of this document but is used here for informational purposes only.

[5] The term "gallery" is sometimes used by entities when referring to the resulting candidate list. For the purposes of this document, the phrase "list of most likely candidates" will be used.

After the list is generated, trained human examiners follow-up on the list of most likely candidates by performing analysis to compare the probe photograph with the candidate photographs.

While **face recognition** is an automated computer evaluation of similarities between face images, **face comparison** is a manual examination of the differences and similarities between two face images or a live subject and a face image (one-to-one) for the purpose of determining whether they represent the same or different persons. The process is used in concert with standard investigative techniques.

2. Are Face Recognition Results Considered an Identification?

Face recognition search results are not considered positive identification and do not establish probable cause, without further investigation; rather, they are advisory in nature as an investigative lead only. Any possible connection or involvement of an individual to a criminal investigation must be determined through further analysis and investigation.

3. Is Face Recognition Information Considered Criminal Intelligence?

The policy template in Chapter II was developed to articulate entity policies and P/CRCL protections for the collection, receipt, access, use, dissemination, retention, and purging of face recognition information that is ***not yet*** part of a criminal intelligence or investigative file. If, after completing the analytic process, face recognition information is downloaded into a criminal intelligence or investigative file, the information is then considered criminal intelligence or investigative information and the laws, regulations, and policies applicable to that type of information govern its use.[6]

Law enforcement, fusion centers, criminal intelligence units, and other public safety entities utilize different types of information, such as criminal history, suspicious activity reports (SARs), and criminal intelligence as part of their criminal intelligence or investigative activities. Each type is governed by laws, regulations, and policies to authorize and ensure appropriate collection, receipt, access, use, dissemination, retention, and purging. Face recognition information—probe photographs, image repositories, lists of most likely candidates, etc.—is not considered criminal intelligence,[7] criminal history, or SAR information. As such, the laws, regulations, and policies that specifically apply to those types of situations may not apply to face recognition information ***until*** such time as it is downloaded and incorporated into a criminal intelligence or investigative case file. It is the further analytic and investigative processes by trained examiners that associate face recognition results with an identifiable individual.

B. How to Use This Resource

This resource contains a P/CRCL policy template in Chapter II. The provisions suggested in the template can be incorporated into the entity's general operational policies and day-to-day operations which must provide explicit and detailed P/CRCL protection guidance to entity personnel and other authorized sources

[6] This does not mean that face recognition information is not accorded protections until it is incorporated into a criminal intelligence or investigative file; rather, the provisions of this template were designed to articulate such protections. For example, use and dissemination of face recognition is addressed in Chapter II, Section F. Use of Face Recognition Information, and Section G. Sharing and Disseminating Face Recognition Information.

[7] The operating principles of 28 CFR Part 23 provide guidance to law enforcement regarding how to effectively operate criminal intelligence information systems while safeguarding P/CRCL. The regulation applies, as a matter of law, to state, local, tribal, or territorial agencies if they are operating interjurisdictional or multijurisdictional criminal intelligence systems that are supported with Omnibus Crime Control and Safe Streets Act funding. See 28 CFR Part § 23.3. For participating or member agencies, the intelligence project's operating policies, as set forth in a participation or membership agreement, govern their submission, access, use, retention/destruction, and any third-party dissemination of criminal intelligence information received from the intelligence project. For further information, see https://28cfr.iir.com/Resources/Executive-Order. Those entities that are not subject to 28 CFR Part 23 may voluntarily adopt the protections articulated in 28 CFR Part 23 as a matter of policy.

and participating agencies. Each section of the template is a fundamental component of an overall comprehensive face recognition policy.

The template in Chapter II groups policy concepts together (e.g., governance, accountability, security, etc.) into categories, with each category containing policy provisions that relate to that category. Policy provisions are presented as questions to the policy drafter and the drafter then answers by writing policy language, working through each question to build a complete policy. Policy questions and guidance and best practices are shown in **bold type**. To assist policy authors in drafting a policy, sample policy language is provided below each bolded question in regular type, as follows:

> **1. A bolded policy question that the entity will answer with written policy provisions.**
>
> **Notes and best practices are also shown under each question in bold.**
> **[Special instructions, if any, are bolded and bracketed under each question.]**
>
> Sample policy language is provided underneath each policy question in plain text. If used, this language MUST be customized by filling in the bracketed items, such as the **[name of the entity]**.

In addition, throughout the template, several terms are **underlined and hyperlinked** to their definitions in Appendix A. Glossary of Terms and Definitions, to assist policy drafters in understanding the terminology used.

1. Program Versus System

To aid in the reader's understanding, the following describes this resource's use of the terms "face recognition program" and "face recognition system."

- **Face Recognition Program**—A term used in this resource to describe an entity's face recognition initiative, which includes the management of human components (management, analysts, examiners, authorized users), ownership and management of the face recognition system (technical components, see below), and the establishment and enforcement of entity-wide processes, policies, and procedures.
- **Face Recognition System—**A term used in this resource to describe the technical components of a face recognition program, such as hardware, software, interfaces, image repositories, templates, autogenerated candidate lists, etc. While some entities own such a system (see above), others may have authorized access to another entity's face recognition system.

2. What Entities Should Use the Policy Template?

The policy template, contained in Chapter II, is designed for use by state, local, tribal, and territorial (SLTT) law enforcement entities, fusion centers, and other public safety agencies that either own and operate their own face recognition program or only have direct access to, and authorized use of, another entity's face recognition system. Entities are guided to adopt and customize the provisions of the template that apply to the entity's face recognition system or program.

An entity must set forth in a formalized agreement, such as a memorandum of understanding (MOU) or interagency agreement, the essential requirements for submitting face recognition search requests by external agencies to the entity. The policy provisions in Chapter II's template may be useful to inform the key components of the formalized agreement. For example, the entity may require requesting agencies to complete specialized training, as referenced in Chapter II, Section N. Training, item 4.

3. Transparency and Referencing Other Policies

Frequently, agencies already have established privacy-related policies and procedures that may be contained in broader policy documents (e.g., concept of operations, standard operating procedures, user agreements, and employee handbooks). There may also be cross over between the provisions in this template and other policies, such as an entity's social media or general privacy policy. In accordance with Chapter II, Section M. Accountability and Enforcement, and Subsection M.1. Transparency, agencies are strongly encouraged to make their face recognition policies available to the public, even if the other existing policies or procedures are not made publicly available.

Agencies are cautioned against providing cross-references within their face recognition policies to policy provisions contained in other policies that are not available to the public, without excerpting the relevant text. Providing a cross-reference to, for example, a numbered section (e.g., "policy number 201.56-B, section 6.a.") within a non-publicly available policy, without excerpting the relevant text will confuse the reader (e.g., if the reader is not an employee and does not have access to policy 201.56-B). As such, the reader will not know what is meant by the numeric cross-reference. For this reason, it is better to excerpt (or restate) the actual language of the specific policy provision the entity wants to emphasize within the face recognition policy. As a best practice, only cross reference policies that are publicly available or restate (excerpt) the applicable language within the face recognition policy.

CAUTION

Do not assume that an existing policy (for example, on fingerprints) will automatically apply to other biometric technologies without a thorough assessment of similarities and differences of biometrics, regulations, etc.

4. Mobile Face Recognition Use

Mobile face recognition applications generally use an image of an individual, which is captured in the presence of a law enforcement officer in the field. Then, using a mobile interface, the image is submitted as a probe photograph to search image repositories, which can result in a list of most likely candidate images. Trained law enforcement officers evaluate the candidate images using standard investigative techniques to make a determination of whether the person in front of them is an individual shown in the candidate result listing.

Law enforcement use of mobile face recognition devices and applications is an area where public concern has been raised. This resource does not take an official position on mobile use of this technology. However, it is highly recommended that if an entity makes a decision to implement and utilize mobile face recognition applications, it should do so **only** after vetting the decision, requiring appropriate training for officers who are authorized to capture remote face images and use mobile search applications, and developing comprehensive policies to address such use. To assist entities in policy development to specifically address mobile use of this technology, the following provisions were added to the policy template and are contained in Chapter II of this resource.

- Section A, Purpose Statement, provision number 3
- Section F, Use of Face Recognition Information, provision number 6
- Section F, Use of Face Recognition Information, provision number 7
- Section F, Use of Face Recognition Information, provision number 8
- Section N, Training, provision number 5

Additional face capture training and other provisions may also be needed, depending on the entity's unique use of this technology in the field. If the entity does not utilize mobile face recognition, these provisions will not apply when the entity is developing a non-mobile face recognition policy. Another option is for the entity to add policy provisions that specifically articulate the entity's exclusion of mobile face recognition use. Either choice is acceptable. What is important is the entity develop a face recognition policy that accurately describes its operations and compliance with applicable laws, regulations, policies, rules, or other constraints in all uses of the technology.

5. Face Recognition Analysis on Live Video

Face recognition analysis on live video is different than mobile face recognition. While mobile face recognition entails using a mobile device to capture a photo of a subject who is in the presence of a law enforcement officer, such as during a traffic stop, face recognition analysis on live video means that face recognition searches may be performed on images of any individual captured within the frame of a live feed video camera (such as a closed circuit television).

It is important for the entity to articulate a clear and affirmative statement regarding the entity's position regarding face recognition analysis on live video. To assist entities during policy development, provision F. Use of Face Recognition Information, item 3., was added to the policy template, in Chapter II of this resource, to specifically address face recognition analysis on live video.

6. Template Modifications—Customizing Your Policy

It is important to note that the policy development template in Chapter II **is not intended to be used as is** without modification. Nor is it intended to create inconsistencies with applicable laws and regulations. The sections represent the suggested foundational components of an effective face recognition policy but do not cover all situations, processes and procedures, or the applicable constitutional provisions, laws, ordinances, or regulations that may be unique within your state. The template represents a starting point for your entity to establish baseline face recognition policy guidelines. Law enforcement and public safety entities are encouraged to complete as many of the template questions as are applicable; to enhance sections to include items such as references to applicable statutes, rules, standards, or policies; and to add sections for provisions that are not addressed in the template.

To facilitate this process, the following appendices have been developed for review and customization, as appropriate, and should be referenced in each entity's face recognition policy:

- Appendix A—Glossary of Terms and Definitions
- Appendix B—Fair Information Practice Principles (FIPPs)
- Appendix C—Listing of Federal Laws

It is important that entities review each of the policy questions, as well as the notes, references, and instructional information provided with each, when drafting entity policy language. However, to assist entities in the drafting and customization process, all of the sample policy language contained in the template has been extracted and provided in Appendix D, Sample Face Recognition Policy.

C. Resource List

The following list provides useful face recognition and biometric-related resources, policy development templates, privacy regulations and authorities, and other resources that may be of interest:

1. Face Recognition and Biometric-Related Resources

- ***Biometric Specifications for Personal Identity Verification***, NIST Special Publication 800-76-2, National Institute of Standards and Technology (NIST), U.S. Department of Commerce, July 2013, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-76-2.pdf.

- ***Capture and Equipment Assessment for Face Recognition Systems***, Version 1.0, Facial Identification Scientific Working Group (FISWG), May 5, 2011, https://www.fiswg.org/FISWG_CaptureAndEquipmentAssessmentForFRSystems_v1.0_2011_05_05.pdf.

- ***Data Format for the Interchange of Fingerprint, Facial, and Other Biometric Information***, 2011 American National Standard for Information Systems, Information Technology Laboratory (ITL),

American National Standards Institute/National Institute of Standards and Technology (ANSI/NIST), Update 2015, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-290e3.pdf.

- ***Electronic Biometric Transmission Specification*** (EBTS), NGI-DOC-01862-x.x., Criminal Justice Information Services (CJIS), Federal Bureau of Investigation (FBI), www.fbibiospecs.cjis.gov.

- **Face Recognition Challenges and Evaluations** (FaCE), NIST, https://www.nist.gov/programs-projects/face-challenges.

- **Face Recognition Technology (FERET) Program**, Department of Defense (DoD) Counterdrug Technology Development Program Office, https://www.nist.gov/programs-projects/face-recognition-technology-feret.

- **Face Recognition Vendor Test (FRVT)**, NIST, https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt.

- **FRVT—Performance of Automated Gender Classification Algorithms**, NIST Interagency/Internal Report (NIST IR) – 8052, April 2015, https://www.nist.gov/publications/face-recognition-vendor-test-frvt-performance-automated-gender-classification.

- **FRVT—Performance of Face Identification Algorithms**, NIST IR 8009, May 21, 2014, https://www.nist.gov/publications/face-recognition-vendor-test-frvt-performance-automated-gender-classification.

- ***Facial Comparison Overview***, Version 1.0, FISWG, April 29, 2010, https://www.fiswg.org/FISWG_Facial_Comparison_Overview_v1.0_2010.04.29.pdf.

- **Facial Identification Scientific Working Group**, https://www.fiswg.org/.

- ***Facial Image Comparison Feature List for Morphological Analysis***, Version 1.0, FISWG, November 22, 2013, https://www.fiswg.org/FISWG_1to1_Checklist_v1.0_2013_11_22.pdf.

- ***Facial Recognition System: Methods and Techniques***, Version 1.0, FISWG, August 13, 2013, https://www.fiswg.org/FISWG_fr_systems_meth_tech_v1.0_2013_08_13.pdf.

- ***Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies***, Federal Trade Commission, October 2012, https://www.ftc.gov/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies.

- ***Glossary***, Version 1.1, FISWG, February 2, 2012, https://www.fiswg.org/FISWG_Glossary_v1.1_2012_02_02.pdf.

- ***Guidelines for Facial Comparison Methods***, Version 1.0, FISWG, February 2, 2012, https://www.fiswg.org/FISWG_GuidelinesforFacialComparisonMethods_v1.0_2012_02_02.pdf.

- ***Information Technology: American National Standard for Information Systems-Data Format for the Interchange of Fingerprint, Facial, & Other Biometric Information***, NIST Special Publication 500-290, November 2011, http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=910136.

- ***Information Technology—Vocabulary—Part 37:Biometrics***, International Standard, International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), ISO/IEC 2382-37, Second edition, February 2017, http://standards.iso.org/ittf/PubliclyAvailableStandards/c066693_ISO_IEC_2382-37_2017.zip.

- ***Photograph Finish—Your Mug Shots Should Look Much Like This***, April 9, 2014, CJIS link, Criminal Justice Information Services (CJIS), Federal Bureau of Investigation (FBI), https://www.fbi.gov/services/cjis/cjis-link/photo-finish-your-mug-shots-should-look-much-like-this.

- ***Privacy and Information Quality Risks: Justice Agency Use of Biometrics***, Global Justice Information Sharing Initiative (Global), Bureau of Justice Assistance (BJA), Office of Justice Programs (OJP), U.S. Department of Justice (DOJ), September 1, 2011, http://it.ojp.gov/gist/77/Privacy-and-Information-Quality-Risks--Justice-Agency-Use-of-Biometrics.

- ***Privacy Best Practice Recommendations for Commercial Facial Recognition Use,*** National Telecommunications and Information Administration (NTIA), U.S. Department of Commerce, June 15, 2016, https://www.ntia.doc.gov/files/ntia/publications/privacy_best_practices_recommendations_for_commercial_use_of_facial_recogntion.pdf.

- ***Standards and Guidelines for Forensic Art and Facial Identification,*** International Association of Identification, April 2010, https://www.theiai.org/disciplines/art/ForensicArtGuidelinesSGFAFI1stEd.pdf.

- ***Video Evidence: A Law Enforcement Guide to Resources and Best Practices,*** Global, BJA, OJP, DOJ, March 2014, http://it.ojp.gov/gist/164/Video-Evidence--A-Law-Enforcement-Guide-to-Resources-and-Best-Practices.

2. Policy Development Templates

In addition to this resource, the following policy templates were developed through support of the Global Justice Information Sharing Initiative's Criminal Intelligence Coordinating Council, sponsored by the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice, in collaboration with the U.S. Department of Homeland Security (DHS). Each is designed to assist justice entities in developing P/CRCL policies, including the use of social media and license plate readers in intelligence and investigative activities.

- ***Developing a Policy on the Use of Social Media in Intelligence and Investigative Activities: Guidance and Recommendations***, Global, BJA, OJP, DOJ, February 2013, https://it.ojp.gov/GIST/132/Developing-a-Policy-on-the-Use-of-Social-Media-in-Intelligence-and-Investigative-Activities--Guidance-and-Recommendations-.

- ***Fusion Center Privacy Policy Development: Privacy, Civil Rights, and Civil Liberties Policy Template***, DHS and DOJ, April 2010, https://it.ojp.gov/gist/48/Fusion-Center-Privacy-Policy-Development--Privacy--Civil-Rights--and-Civil-Liberties-Policy-Template.

- ***License Plate Reader Policy Development Template for Use in Intelligence and Investigative Activities***, Global, BJA, OJP, DOJ, February 2017, https://it.ojp.gov/GIST/1197/License-Plate-Reader-Policy-Development-Template-for-Use-in-Intelligence-and-Investigative-Activities.

3. Privacy Regulations and Authorities

Refer to Appendix C for synopses of primary federal laws that an entity should review and, where appropriate, consider citing in the face recognition policy to protect face recognition data and any personally identifiable information later associated with the face recognition information. As face recognition information may be incorporated as only one piece of information into a larger case file, the federal laws described in Appendix C may be applicable.

- Code of Federal Regulations (CFR), Title 28 (28 CFR)—Judicial Administration, Chapter 1—U.S. Department of Justice, Part 23—***Criminal Intelligence Systems Operating Policies***, http://it.ojp.gov/documents/28CFR_Part_23.pdf.

- ***Fair Information Practice Principles***, refer to Appendix B.

- ***Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule: A Guide for Law Enforcement,*** U.S. Department of Health and Human Services (HHS), September 2013, https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/special/emergency/final_hipaa_guide_law_enforcement.pdf.

4. Additional Privacy and Security-Related Resources

- ***Criminal Justice Information Services (CJIS) Security Policy***, Version 5.5, CJISD-ITS-DOC-08140-5.5., June 1, 2016, CJIS, FBI, https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center.

- **Federal Privacy Council**, https://www.fpc.gov/federal-privacy-council/.

- ***Guidelines to Ensure That the Information Privacy and Other Legal Rights of Americans Are Protected in the Development and Use of the Information Sharing Environment*** (ISE Privacy Guidelines), Office of the Program Manager, Information Sharing Environment (ISE), https://www.dni.gov/index.php/ic-legal-reference-book/guidelines-to-ensure-that-the-information-privacy-and-other-legal-rights-of-americans-are-protected-in-the-development-and-use-of-the-information-sharing-environment.

- **Office of Privacy and Civil Liberties, U.S. Department of Justice,** https://www.justice.gov/opcl.

- ***Preparing for and Responding to a Breach of Personally Identifiable Information,*** Office Management and Budget (OMB) Memorandum M-17-12, (January 13, 2017), https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/m-17-12_0.pdf.

- ***Privacy, Civil Rights, and Civil Liberties Audit Guidance for the State, Local, Tribal, and Territorial Intelligence Component***, Global, BJA, OJP, DOJ, September 30, 2015, https://it.ojp.gov/GIST/181/Privacy--Civil-Rights--and-Civil-Liberties-Audit-Guidance-for-the-State--Local--Tribal--and-Territorial-Intelligence-Component.

- ***Recommendations for First Amendment-Protected Events for State and Local Law Enforcement Agencies***, Global, BJA, OJP, DOJ, October 13, 2011, https://it.ojp.gov/GIST/35/Recommendations-for-First-Amendment-Protected-Events-for-State-and-Local-Law-Enforcement-Agencies.

- ***Scenarios for PII Identification and Handling*, Appendix A, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)***, NIST, NIST Special Publication 800-122, April 2010, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf.

D. Acknowledgements

The information contained in this template does not represent the views, opinions, official position, or policies of any sole contributor or agency. Rather, this resource was created through a dynamic and collaborative effort of multiple state, local, and federal law enforcement, privacy, and criminal justice partners, practitioners, and subject-matter experts (SMEs). A special thank-you to the following individuals and agencies that provided valuable contributions in the development and vetting of this resource.

1. Face Recognition Policy Group Members

Chair: **Dawn Diedrich**, Director, Office of Privacy and Compliance, Georgia Bureau of Investigation

Federal Partners

- U.S. Department of Homeland Security (DHS)
  - Office of Intelligence and Analysis, State, Local, Tribal, and Territorial (SLTT) Partner Engagement —**Kevin Saupp**, Director of State and Local Partner Engagement, and **Susan Bower**, Program Manager
  - Privacy Office—**Scott Mathews**, Senior Privacy Analyst for Intelligence
  - Office for Civil Rights and Civil Liberties—**Ayn Crawley**, Director, Civil Rights and Civil Liberties Institute, and **David Demski**, Technology Analyst
  - Homeland Security Information Network (HSIN)—**Maria Petrakis**, Policy Manager
  - Office of Biometric Identity Management (OBIM), part of the National Protection and Programs Directorate—**Anne May**, Program and Management Analyst, and **Brian Pittack**, Program and Management Analyst
  - U.S. Customs and Border Protection, Biometric Exit program—**Brandon Fauquet**, Manager and Program Analyst, Planning, Program Analysis, and Evaluation, Office of Field Operations
- U.S. Department of Justice (DOJ)
  - Bureau of Justice Assistance (BJA), Office of Justice Programs (OJP), DOJ—**John Markovic**, Senior Policy Advisor, Justice Information Sharing Team
  - U.S. Drug Enforcement Administration (DEA)
    - **George Johnson III**, Investigative Tech
    - **Bob Montgomery**, Technical Director, All Native Group
    - **Spring Williams**, Unit Chief, Office of Investigative Technology
  - Federal Bureau of Investigation (FBI)
    - FBI Criminal Justice Information Services (CJIS) Division
    - FBI Terrorist Screening Center (TSC)
    - FBI Office of General Counsel/Privacy and Civil Liberties Unit
  - Office of Privacy and Civil Liberties (OPCL)—**Beth Zelman,** Attorney Advisor
  - Office of the Director for National Intelligence (ODNI), Office of Civil Liberties, Privacy, and Transparency—**Eva Kleederman**, Deputy Chief, and **Brian Ince**, Senior Assistant Civil Liberties, Privacy, and Transparency Officer
- ODNI, Office of Partner Engagement, Information Sharing Environment (PE-ISE)—**Frank Pawlowski**, Senior Law Enforcement Advisor

Biometric Privacy SME

- **Pam Dixon**, Executive Director, World Privacy Forum and member of the Privacy and Policy Expert Group, Biometrics Institute

Fusion Centers

- **Lieutenant Ron Fisher** and **Eric Diggs**, Maryland Coordination and Analysis Center
- **Jimmy Gianato**, Director, Division of Homeland Security and Emergency Management, West Virginia, West Virginia Intelligence Fusion Center

State- and Local-Level Facial Recognition Practitioners

- **Commanding Officer Inspector Joseph Courtesis** and **Sergeant Edwin Coello**, Facial Recognition Program, New York Police Department Real Time Crime Center

- **Special Agent in Charge Terry Cowman**, Iowa Department of Public Safety (Association of State Criminal Investigative Agencies [ASCIA] representative)
- **Detective Sergeant First Class Mark Finnegan**, Information & Intelligence Analysis Bureau, Office of the Regional Operations and Intelligence Center, New Jersey State Police
- **Lieutenant Sam McGhee**, Professional Standards Section, Emergency Services Coordinator, Aurora, Colorado Police Department, (International Association of Chiefs of Police, Homeland Security Committee representative)
- **Major Brian Redd**, Utah Department of Public Safety (ASCIA representative)
- **Pam Scanlon**, Executive Director, Automated Regional Justice Information System

2. Other Contributors

The following individuals were not members of the Face Recognition Policy Group but contributed to the resource through conference calls, policy language development, and template review and vetting.

- **Nelson O. Bunn, Jr.**, Executive Director, National District Attorneys Association (NDAA)
- **Lieutenant Cora Gentry**, Identification Bureau, Arkansas State Police
- **Pete Langenfeld**, Section Manager, Digital Analysis and Identification Section, Michigan State Police
- **Mark Vargo**, States Attorney, Pennington County, Rapid City, South Dakota (NDAA Policy Committee representative)

II. Face Recognition Policy Development Template for State, Local, and Tribal Criminal Intelligence and Investigative Activities

A. Purpose Statement

1. Why did the entity implement a face recognition program or establish access and use of a face recognition system?

Facial recognition technology involves the ability to examine and compare distinguishing characteristics of a human face through the use of biometric algorithms contained within a software application. This technology can be a valuable investigative tool to detect and prevent criminal activity, reduce an imminent threat to health or safety, and help in the identification of persons unable to identify themselves or deceased persons. The **[name of entity]** has **[implemented or, if applicable, established access and use of]** a face recognition **[program or, if applicable, system]** to support the investigative efforts of law enforcement and public safety agencies both within and outside **[state name]**.

2. What is the purpose of establishing a face recognition policy (i.e., what does the entity hope to accomplish in adopting this policy)? Provide a succinct, comprehensive statement of purpose.

It is the purpose of this policy to provide **[name of entity]** personnel with guidelines and principles for the collection, access, use, dissemination, retention, and purging of images and related information applicable to the implementation of a face recognition (FR) program. This policy will ensure that all FR uses are consistent with authorized purposes while not violating the privacy, civil rights, and civil liberties (P/CRCL) of individuals.

Further, this policy will delineate the manner in which requests for face recognition are received, processed, catalogued, and responded to. The Fair Information Practice Principles (FIPPs) form the core of the privacy framework for this policy.

This policy assists **[name of entity]** and its personnel in:

- Increasing public safety and improving state, local, tribal, territorial, and national security.
- Minimizing the threat and risk of injury to specific individuals.
- Minimizing the threat and risk of physical injury or financial liability to law enforcement and others responsible for public protection, safety, or health.

- Minimizing the potential risks to individual privacy, civil rights, civil liberties, and other legally protected interests.
- Protecting the integrity of criminal investigatory, criminal intelligence, and justice system processes and information.
- Minimizing the threat and risk of damage to real or personal property.
- Fostering trust in the government by strengthening transparency, oversight, and accountability.
- Making the most effective use of public resources allocated to public safety entities.

3. What are the entity's authorized uses for face recognition information?[8]

All deployments of the face recognition system are for official use only/law enforcement sensitive (FOUO/LES). The provisions of this policy are provided to support the following authorized uses of face recognition information.

[List any of the following that may be applicable and add any other authorized uses that apply to the entity. Note: Uses must be specifically authorized for your entity and must be in accordance with laws, statutes, policies, and procedures governing the entity.

- **A reasonable suspicion that an identifiable individual has committed a criminal offense or is involved in or planning criminal (including terrorist) conduct or activity that presents a threat to any individual, the community, or the nation and that the information is relevant to the criminal conduct or activity.**
- **An active or ongoing criminal or homeland security investigation.**
- **To mitigate an imminent threat to health or safety through short-term situational awareness surveillance or other means.**
- **To assist in the identification of a person who lacks capacity or is otherwise unable to identify him- or herself (such as an incapacitated, deceased, or otherwise at-risk person).**
- **To investigate and/or corroborate tips and leads.**
- **For comparison to determine whether an individual may have obtained one or more official state driver's licenses or identification cards that contain inaccurate, conflicting, or false information.**
- **To assist in the identification of potential witnesses and/or victims of violent crime.**
- **To support law enforcement in critical incident responses.]**

[For those entities using mobile face image capture devices, there may be narrowly tailored purposes for use. Insert the following language and list the purposes that are applicable, and any others that are relevant, to the entity:

Mobile face image searches may be performed only by an officer who has completed training and only during the course of an officer's lawful duties, in furtherance of a valid law enforcement purpose and in accordance with the conditions set forth in section F.7 (Refer to F. Use of Face Recognition Information, item 7). Some suggested valid law enforcement purposes include:

- **For persons who are detained for offenses that:**
  - **Warrant arrest or citation or**
  - **Are subject to lawful identification requirements and are lacking positive identification in the field.**
- **For a person who an officer reasonably believes is concealing his or her true identity and has a reasonable suspicion the individual has committed a crime other than concealing his or her identity.**
- **For persons who lack capacity or are otherwise unable to identify themselves and who are a danger to themselves or others.**
- **For those who are deceased and not otherwise identified.]**

[8] Entities should reference the classification of information established in entity policies and procedures.

B. Policy Applicability and Legal Compliance

1. What information is subject to the face recognition policy?

This policy was established to ensure that all images are lawfully obtained, including face recognition probe images obtained or received, accessed, used, disseminated, retained, and purged by the **[name of entity]. This policy also applies to:**

- Images contained in a known identity face image repository and its related identifying information,
- **The face image** searching process.
- Any results from face recognition searches that may be accessed, searched, used, evaluated, retained, disseminated, and purged by the **[name of entity].**
- Lawfully obtained probe images of unknown suspects that have been added to unsolved image files (refer to section L.3), pursuant to authorized criminal investigations.

2. Who is subject to the face recognition policy? Identify who must comply with the face recognition policy; for example, entity personnel, participating agencies, and private contractors.

All **[name of entity]** personnel, participating agency personnel, and authorized individuals working in direct support of **[name of entity]** personnel (such as interns), personnel providing information technology services to the **[name of entity]**, private contractors, and other authorized users will comply with the **[name of entity]**'s face recognition policy and will be required to complete the training referenced in section N.2. In addition, authorized **[name of entity]** personnel tasked with processing face recognition requests and submissions must also complete the specialized training referenced in section N.3. An outside agency, or investigators from an outside agency, may request face recognition searches to assist with investigations only if **[insert applicable requirement(s) from those recommended below or insert the entity's established requirements:**

- **Prior to making requests, the outside agency has a formalized agreement (e.g., a memorandum of understanding or an interagency agreement) between the [name of entity] and the outside agency and the agreement acknowledges that requesting investigators have an understanding of the training concepts listed in section N. Training, item 4.**
- **The outside agency first provides examples of its applicable policies (e.g., privacy) and acknowledges in writing that its requesting investigators have an understanding of the training concepts listed in section N. Training, item 4.**
- **The outside agency completes the [name of entity]'s training identified in section N. Training, item 4.**
- **The outside agency is a law enforcement agency that is making the request based on a valid law enforcement purpose that falls within the authorized uses listed in section A. Purpose Statement, item 3. and the requestor provides a case number and contact information (requestor's name, requestor's agency, address, and phone number) and acknowledges an agreement with the following statement:**

  The result of a face recognition search is provided by the [name of entity] only as an investigative lead and IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT. Any possible connection or involvement of any subject to the investigation must be determined through further investigation and investigative resources.]

3. How is the entity's face recognition policy made available to personnel, participating entities, and individual users (e.g., in print, online, etc.), and does the entity require acknowledgment, in writing, of receipt and agreement to comply with this policy?

The **[name of entity]** will provide a printed or electronic copy of this face recognition policy to all:

- **[name of entity]** and non-**[name of entity]** personnel who provide services
- Participating agencies
- Individual authorized users

The **[name of entity]** will require both a written acknowledgement of receipt of this policy and a written agreement to comply with this policy and its applicable provisions.

4. **This entity requires *personnel and participating information-originating and user agencies* to be in compliance with all applicable constitutional and statutory laws. What are the primary laws with which personnel and participating agencies must comply?**

   Cite the primary laws with which personnel and participating users must comply that protect privacy, civil rights, and civil liberties (P/CRCL) in the collection, receipt, access, use, dissemination, retention, and purging of face recognition information.

   This should include any statute enacted by state or local government regarding deployed face recognition systems by affiliated entities. It might also include relevant provisions of the U.S. Constitution and state constitutions; open records or sunshine laws; information breach notification laws; other laws, regulations, orders, opinions, or policies impacting or protecting P/CRCL; local ordinances; and relevant federal laws, such as the Driver's Privacy Protection Act and regulations. (For synopses of primary federal laws, refer to Appendix C, Listing of Federal Laws.)

   All **[name of entity]** personnel, participating agency personnel, and authorized individuals working in direct support of **[name of entity]** personnel (such as interns or volunteers), personnel providing information technology services to the **[name of entity]**, private contractors, agencies from which **[name of entity]** information originates, and other authorized users will comply with applicable laws and policies concerning P/CRCL, including, but not limited to **[include a specific reference to any relevant state statutes or other binding state or local policy specific to face recognition systems, then provide a list of other applicable state and federal P/CRCL laws and/or include a reference to the section or appendix containing a list of applicable laws]**.

C. Governance and Oversight

1. **Who has primary responsibility for the entity's overall operation, including the entity's justice information systems, face recognition program and system, information collection and retention procedures, coordination of personnel, and enforcement of this policy? Which individual will ultimately be held accountable for any problems or errors?**

   Primary responsibility for the operation of the **[name of entity]**'s justice information systems, face recognition program and system, operations, and the coordination of personnel; the receiving, seeking, retention, evaluation, data quality, use, purging, sharing, disclosure, or dissemination of information; and the enforcement of this policy is assigned to the **[position/title]** of the **[name of entity]**.

2. **Who is assigned primary responsibility for overseeing and administering the entity's face recognition program?**

   The **[name of entity]**'s **[insert title]** will designate **[a face recognition administrator or face recognition unit or department who/that]** will be responsible for the following **[include any of the following responsibilities that apply to the face recognition administrator or other responsibilities:**
   - **Overseeing and administering the face recognition program to ensure compliance with applicable laws, regulations, standards, and policy.**
   - **Acting as the authorizing official for individual access to face recognition information.**
   - **Ensuring that user accounts and authorities granted to personnel are maintained in a current and secure "need-to-know" status.**
   - **Reviewing face recognition search requests, reviewing the results of face recognition searches, and returning the most likely candidates—or candidate images—if any, to the requesting agency.**

- **Ensuring that protocols are followed to ensure that face recognition information (including probe images) is automatically purged in accordance with the entity's retention policy (refer to section L.1. Information Retention and Purging), unless determined to be of evidentiary value.**
- **Ensuring that random evaluations of user compliance with system requirements and the entity's face recognition policy and applicable law are conducted and documented (refer to section M.2. Accountability).**
- **Confirming, through random audits, that face recognition information is purged in accordance with this policy and to ensure compliance with applicable laws, regulations, standards, and policy.**
- **Ensuring and documenting that personnel (including investigators from external agencies who may make face recognition search requests) meet all prerequisites stated in this policy prior to being authorized to use the face recognition system.]**

3. **What is the operating entity's role with regard to the face recognition program?**

   [Select the option that is applicable to the entity.]

   Option 1: The entity operates its own face recognition program.

   The **[name of entity]** face recognition program was established on **[date]** in conjunction with **[other agency partners, if applicable]**. Personnel from the following agencies are authorized to request face recognition searches:
   - **[Insert list of agencies authorized to request face recognition searches]**.

   Option 2: The entity has authorized access to a face recognition system.

   The **[name of entity]** has authorized access to and can perform face recognition searches utilizing the **[insert name of entity that owns the face recognition program]** face recognition system.

4. **Is there is a commercial entity or vendor involved and, if so, what is that vendor's role?**

   The **[name of entity]** contracts with **[insert name of commercial entity or vendor]** to provide **[insert applicable vendor role, such as "software and system development services for the entity's face recognition system"]**. The **[name of entity]** retains ownership of the face recognition system and the images and information it contains.

5. **What is the process for developing, reviewing, and updating the face recognition policy?**

   The **[name of entity]** is guided by a **[insert guiding authority, for example, a "designated face recognition oversight committee"]** that ensures that P/CRCL are not violated by this face recognition policy and by the **[name of entity]**'s face recognition information collection, receipt, access, use, dissemination, retention, and purging processes and procedures. The **[insert guiding authority, for example, a "designated face recognition oversight committee"]** engages with the community regarding **[name of entity]'s** face recognition policy prior to publishing.

   It is suggested that the committee will annually review and update the face recognition policy in response to changes in law and program implementation experience, including the results of audits and inspections, and may ***solicit input from the entity's stakeholders*** **[insert, if applicable "and may provide notice to and solicit comment from the public"]** on the development of the face recognition policy or proposed updates to the face recognition policy.

6. **Who is the designated and trained privacy officer (or entity) who will handle reported errors and violations of this policy and who will oversee the implementation of this policy and face recognition P/CRCL protections?**

[Provide the title of the individual or name of the entity. This may be the privacy officer; legal counsel; internal affairs; external entities such as the U.S. Attorney or the Office of Inspector General; or other personnel who have independent authority to perform oversight responsibilities.]

The **[insert title of individual or name of entity]** will:

- Receive reports regarding alleged errors and violations of the provisions of this face recognition policy or applicable state law.
- Receive and coordinate complaint resolution under the [name of entity]'s face recognition redress policy.
- Ensure that the provisions of this policy and P/CRCL protections are implemented through efforts such as training, business process changes, and system designs that incorporate privacy-enhancing technologies.

The **[insert title of individual but not the name or name of entity]** may be contacted at the following address: **[insert phone number, mailing address, or e-mail address]**, which is also posted on **[insert website where this information is listed for purposes of public redress]**.

7. **Who, or what entity, is responsible for ensuring that enforcement procedures and sanctions for noncompliance with the face recognition policy are adequate and enforced?**

   The **[insert title of individual or name of entity]** will ensure that enforcement procedures and sanctions outlined in **[insert section number of policy (see Section M.3. Enforcement)]** are adequate and enforced.

D. Definitions

1. **What key words or phrases are regularly used in the face recognition policy for which the entity wants to specify particular meanings?**

   This may include terms that are not commonly known or have multiple meanings that may need to be clarified to indicate which one applies to the face recognition policy. There may be legal definitions for terms in the statutes governing the operation of justice information or face recognition systems or programs. For examples of definitions of key terms commonly used throughout this template, refer to Appendix A, Glossary of Terms and Definitions.

   For examples of primary terms and definitions used in this face recognition policy, refer to **[insert section or appendix citation]**.

E. Acquiring and Receiving Face Recognition Information

1. **What image repositories are searched using the entity's face recognition system? Select all options that are applicable to the entity.**

   Option 1: The entity maintains or operates an entity-owned image repository.

   The **[name of entity]** face recognition system can access and perform face recognition searches utilizing the following entity-owned face image repositories:

   - **[Insert a list of entity-owned and maintained repositories, including information types.]**

Option 2: The entity has authorized access to and can perform face recognition searches utilizing image repositories not owned by the entity. Indicate the authority/source of the repository (e.g., driver's license images).

The **[name of entity]** is authorized to access and perform face recognition searches utilizing the following external repositories:

[List the image type and authority/source for each repository accessed. These may include:

- **Mug-shot images [check state authority and insert source]**
- **Driver's license photographs [check state authority and insert source]**
- **State identification card photographs [check state authority and insert source]**
- **Sex Offender Registry [check state authority and insert source]**
- **[Specify any other image repositories that are accessed and cite state authority.]]**

Option 3: In addition to the above, the entity is authorized to request that face recognition searches be performed by an external entity that operates a face recognition program.

In addition to above, the **[name of entity]** is authorized to submit requests for face recognition searches to be performed by the following external entities that own and maintain face image repositories:

[List the image type and authority/source for each repository accessed. These may include:

- **Mug-shot images [check relevant state law and insert source]**
- **Driver's license images [check relevant state law and insert source]**
- **State identification card images [check relevant state law and insert source]**
- **Sex Offender Registry [check relevant state law and insert source]**
- **[Specify any other image repositories that are accessed and cite state authority.]]**

2. **For use in performing a face recognition search, describe the conditions under which the entity will obtain or accept probe images. Note: State and federal law and/or policies may restrict queries to commercial repositories.**

   For the purpose of performing face recognition searches, the **[name of entity]** and authorized **[name of entity]** personnel will obtain probe images or accept probe images from authorized requesting or participating agencies only for the authorized uses identified in A. 2.

3. **If the entity receives probe images from other law enforcement agencies, identify the mechanism by which this occurs (e.g., memorandum of understanding [MOU], law, intergovernmental agreement [IGA]).**

   The **[name of entity]** will receive probe images only from **[list other law enforcement agency or agencies]** in accordance with **[insert mechanisms, e.g., MOU, law, intergovernmental or interagency agreement]** established between the **[name of entity]** and the law enforcement agency(ies). If a non-law enforcement entity wants to submit a probe image for the purpose of a face recognition search, the entity will be required to file a criminal complaint with the appropriate law enforcement entity prior to the search.

4. **Identify the federal or state constitutional prohibitions or prohibitions in federal, state, local, or tribal laws under which the entity and/or participating agencies will not request or perform face recognition searches.**

   Best Practice: Entities should consider an additional level of review and approval in order to enhance protection and ensure appropriate use of this technology in sensitive locations or populations.

The **[name of entity]** and, if applicable, any authorized requesting or participating agencies will not violate First, Fourth, and Fourteenth Amendments and will not perform or request face recognition searches about individuals or organizations based solely on their religious, political, or social views or activities; their participation in a particular noncriminal organization or lawful event; or their races, ethnicities, citizenship, places of origin, ages, disabilities, genders, gender identities, sexual orientations, or other classification protected by law.

However, the **[name of entity]** accords special consideration to the collection of face images relating to First Amendment-protected events, activities, and affiliations. Because of the sanctity of the First Amendment, law enforcement's role at First Amendment-protected events is usually limited to crowd control and public safety.[9] If, however, during the planning assessment and approval process for the particular event, before proceeding with the collection, the **[name of entity]** anticipates a need for the collection of face images, the **[name of entity]** will articulate whether collection of face images by law enforcement officers at the event is permissible; the legal or justified basis for such collection (including specifics regarding the criminal behavior that is suspected); and how face images may be collected, used, or retained, in accordance with this policy, as appropriate. If face images will be collected, the plan will specify the type of information collection that is permissible, identify who will collect face images (uniform or plainclothes officers), and define the permissible acts of collection.

[Note: Some law enforcement purposes may be stated generally in the Operations Plan or communicated to officers, but objectives that may risk interference with the exercise of First Amendment rights should be stated narrowly and be expressly tied to a specific law enforcement function (e.g., public safety, investigative).]

The use of mobile face image capture devices relating to First Amendment-protected events, activities, and affiliations will be specially authorized by **[title of entity supervisor/director/administrator]** of the **[name of entity]** in advance of the event.

The **[name of entity]** will reassess the need for and use of face recognition during the First Amendment-protected event. The **[name of entity]** will utilize face images from a First Amendment-protected event should the public safety mission change or in support of an active or ongoing criminal or homeland security investigation that occurs during or resulted from a First Amendment-protected event.

5. **If the entity contracts with a commercial face recognition vendor, does the entity require an assurance that the vendor or subcontractor is in legal compliance in its information collection, receipt, access, retention, dissemination, and purging procedures?**

   The **[name of entity]** will contract only with commercial face recognition companies or subcontractors that provide assurances that their methods for collecting, receiving, accessing, disseminating, retaining, and purging face recognition information comply with applicable local, state, tribal, territorial, and federal laws, statutes, regulations, and policies and that these methods are not based on unfair or deceptive information collection practices.

F. Use of Face Recognition Information

1. **Describe the authorized access to or disclosure of face recognition search results *within the entity or in other governmental agencies*. Entities may consider developing policies for addressing use of face recognition in conjunction with certain "sensitive" locations or populations (e.g., places of worship, academia). In addition, indicate if the entity has certain restrictions or allowances for the use of images in briefings or trainings, and whether there are any distinctions for hard copy versus digital images.**

[9] For further information about these processes, see *Recommendations for First Amendment-Protected Events for State and Local Law Enforcement Agencies* at 4, Global Justice Information Sharing Initiative, https://it.ojp.gov/GIST/35/Recommendations-for-First-Amendment-Protected-Events-for-State-and-Local-Law-Enforcement-Agencies.

<u>Best Practice</u>: Entities should consider an additional level of review and approval in order to enhance protection and ensure appropriate use of this technology in sensitive locations or populations.

Access to or disclosure of face recognition search results will be provided only ***to individuals within the entity or in other governmental agencies*** who are authorized to have access and have completed applicable training outlined in section N. Training, and only for valid law enforcement purposes (e.g., enforcement, reactive investigations), and to IT personnel charged with the responsibility for system administration and maintenance. Authorized uses are described in A.3 of this policy. [**Insert, if applicable, any additional restrictions or allowances regarding the use of images in briefings or trainings, and whether there are any distinctions for hard-copy versus digital images.]**

2. **For what purposes does the entity prohibit accessing and using the <u>face recognition system</u> and disseminating face recognition search results?**

   The **[name of entity]** will prohibit access to and use of the face recognition system, including dissemination of face recognition search results, for the following purposes:
   - Non-law enforcement (including but not limited to personal purposes).
   - Any purpose that violates the U.S. Constitution or laws of the United States, including the protections of the First, Fourth, and Fourteenth Amendments.
   - Prohibiting or deterring lawful individual exercise of other rights, such as freedom of association, implied by and secured by the U.S. Constitution or any other constitutionally protected right or attribute.
   - Harassing and/or intimidating any individual or group.
   - Any other access, use, disclosure, or retention that would violate applicable law, regulation, or policy.

3. **Does the entity allow face recognition analysis on live or recorded video?**

   <u>Best Practice</u>: It is important for the entity to articulate a clear and affirmative statement regarding the entity's position regarding face recognition analysis on live or recorded video.[10]

   The **[name of entity] [does not/does]** connect the face recognition system to any interface that performs live video surveillance, including surveillance cameras, drone footage, and body-worn cameras. The face recognition system **[will not/will]** be configured to conduct face recognition analysis on live or recorded video.

4. **What types of user actions and permissions are controlled by the entity's face recognition access limitations?**

   <u>Best Practice</u>: Least privilege administration is a recommended security practice in which every user is provided with only the minimum privileges needed to accomplish the tasks he or she is authorized to perform. It is suggested that entities specify their method for identifying user actions and permissions as it relates to face recognition information within their face recognition policies.

   The **[name of entity]** will employ credentialed, role-based access criteria, as appropriate, to control:
   - Categories of face recognition information to which a particular group or class of users may have access, based on the group or class.
   - The assignment of roles (e.g., administrator, manager, operator, and user).
   - The categories of face recognition information that a class of users are permitted to access, including information being utilized in specific investigations.

[10] Face recognition analysis on live video is different than mobile face recognition. While mobile recognition entails using a mobile device to capture a photo of a subject who is in the presence of a law enforcement officer (e.g., during a traffic stop), face recognition analysis on live video means that face recognition searches may be performed on images of any individual captured within the frame of a live feed video camera (such as a closed circuit television).

- Any administrative or functional access required to maintain, control, administer, audit, or otherwise manage the information or equipment.

5. What is the entity's standard face recognition search procedure?

The following is a suggested sample procedure which should be customized by the entity to reflect its actual face recognition search standard procedures. Each agency will determine which of the following steps, and others, are necessary to support its various operations, acknowledging that each step may not be executed (e.g., using a filtered search as a secondary search) in every instance.

Note: Entities are encouraged to refer to the National Institute of Standards and Technology's (NIST) Face Recognition Vendor Test (FRVT) Ongoing website for information on matching algorithms from independent government evaluations of commercially available and prototype face recognition technologies at https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt-ongoing.

The following describes the **[name of entity]**'s manual and automated face recognition search procedure, which is conducted in accordance with a valid law enforcement purpose and this policy.

- Authorized **[name of entity]** personnel **[and/or authorized requesting agency personnel]** will submit a probe image of a subject of interest.
- Trained **[name of entity]** authorized examiners will initially run probe images without filters, using a filtered search as a secondary search, if needed. In some cases, enhancements may be considered after running an image as is against the image repository.
- In the automated search, most likely candidates are returned to the requestor ranked in order based on the similarity or confidence level.
- The resulting candidates, if any, are then manually compared with the probe images and examined by an authorized, trained examiner. Examiners shall conduct the comparison of images, biometric identifiers, and biometric information in accordance with their training.
    - If no likely candidates are found, the requesting entity will be informed of the negative results. In the case of a negative result, the images examined by the examiner will not be provided to the requesting entity.
- Examiners will submit the search and subsequent examination results for a peer review of the probe and candidate images for verification by other authorized, trained examiners.
- All results of most likely candidate images from the face recognition search must be approved by a supervisor prior to dissemination.
- All entities receiving the results of a face recognition search, must be cautioned that the resulting candidate images do not provide positive identification of any subject, are considered advisory in nature as an investigative lead only, and do not establish probable cause, without further investigation, to obtain an arrest warrant without further investigation.
- The following statement will accompany the released most likely candidate image(s) and any related records:

  The **[name of entity]** is providing this information as a result of a search, utilizing face recognition software, of records maintained by the **[name of records entity]**. This information is provided only as an investigative lead and **IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT**. Any possible connection or involvement of any subject to the investigation must be determined through further investigation and investigative resources.

6. Does the entity operate a mobile face recognition search capability and, if so, what is the process?

The **[name of entity]** has established the following process for mobile face recognition searches:

- Only **[name of entity]** authorized and trained officers may utilize the mobile face recognition application and only on department-authorized devices. **[If personal devices are permitted, insert entity policy regarding use of mobile face recognition on personal devices.]**

- Prior to utilizing a face recognition search, an officer should first attempt to ascertain an individual's identity by means other than a face recognition search, such as requesting identification, using a fingerprint scanner, etc.
- Mobile searches may be performed during the course of an officer's lawful duties and only for the entity-established authorized uses listed in section A. Purpose Statement, item 3.
- In addition, officers may only capture an individual's image when one of the conditions listed in section F.7 exist.
- **[Use the following language, if the process is applicable to the entity. "The face recognition system does not work over standard cellular internet. Officers must log in and be authenticated into the [name of entity]'s law enforcement network in order to access the face recognition system."]**
- The log-in screen will prompt the user to acknowledge and agree to the following statement before granting access to the system:
  - Face recognition is not a form of positive identification of a subject. Images returned as a result of a face recognition search may be considered investigative lead information only and are not probable cause to arrest, without further investigation.
  - Face recognition searches shall not be performed by the user on behalf of others who have not been trained and authorized to perform the searches.
  - All face recognition searches are subject to audit and require case numbers and file class/crime types.
  - Misuse may result in administrative and/or criminal penalties.
- Prior to executing the search, the officer must enter the reason for the search within the application. **[List the reasons that are prompted by the entity's face recognition application. Reasons may include the following:**
  - **Consent**
  - **Reasonable suspicion of a crime**
  - **Probable cause**
  - **Physical/mental incapacity**
  - **Test/training**
  - **Other—[enter written reason]**
- The captured image (probe image) will be submitted to the face recognition system, which will compare the probe image with those contained in the **[indicate the name(s) of repository/ies searched]**.
- A list of most likely candidate images is returned ranked by computer-evaluated similarity.
- The officer then completes a visual or manual morphological comparison of the candidate images with the subject's probe image to make a visual judgment, as well as uses standard investigative techniques, to determine whether the subject is the same as a candidate image.

7. What are the conditions by which a mobile face recognition search may be conducted?

Authorized and trained **[name of entity]** officers may only perform a mobile face recognition search during the course of lawful duties, in accordance with entity-established authorized uses (refer to section A. Purpose Statement, item 3), and when one of the following conditions exist:

- Public Place: In accordance with applicable law, the individual's image is captured in a public place for the purpose of identification and the individual has no reasonable expectation of privacy. The **[name of entity]** will not authorize the collection of the individual's face image when the individual raises an objection that is recognized by law (e.g., religious objection).
- Consent: The individual consents to have his or her image captured for the purpose of identification. The individual may withdraw consent at any time. If consent is withdrawn and neither of the other conditions applies, then use of a face recognition search is not authorized and the search must stop immediately.
- Incapacitation, Defect, or Death: When an individual is unable to provide reliable identification because of physical incapacitation or defect, mental incapacitation or defect, or death, and an immediate identification is needed to assist the officer in the performance of his or her lawful duties.

8. **When, if ever, is force used to capture a subject's image?**

   At no time is the use of force permitted to capture a subject's image.

G. Sharing and Disseminating Face Recognition Information

1. **What requirements must be met before external law enforcement agencies can request face recognition searches?**

   The **[name of entity]** will establish requirements for external law enforcement agencies to request face recognition searches. These will be documented in an interagency agreement or MOU, which will include an assurance from the external agency that it complies with the laws and rules governing it, including applicable federal and state laws. The agreement will specify only those agency personnel who have been authorized by the **[name of entity]**, who have completed the required training identified in section N.2, and that requests are for official use only/law enforcement sensitive (FOUO/LES). Each request must be accompanied by a complaint number or case number.

2. **Under what circumstances will the entity or contracted vendor *not disclose* face recognition information?**

   The **[name of entity]**'s face recognition search information **will not** be:
   - Sold, published, exchanged, or disclosed to commercial or private entities or individuals except as required by applicable law and to the extent authorized by the **[name of entity]**'s agreement with the commercial vendor.
   - Disclosed or published without prior notice to the originating entity that such information is subject to disclosure or publication. However, the **[name of entity]** and the originating agency may agree in writing in advance that the **[name of entity]** will disclose face recognition search information as part of its normal operations, including disclosure to an external auditor of the face recognition search information.
   - Disclosed on a discretionary basis unless the originating agency has provided prior written approval or unless such disclosure is otherwise authorized by the MOU or agreement between the **[name of entity]** and the originating agency.
   - Disclosed to unauthorized individuals or for unauthorized purposes.
   - **[For commercial face recognition vendors, the entity should closely review its vendor agreement.]**

3. **State the entity's policy on confirming the existence or nonexistence of face recognition information to individuals or agencies that are not authorized to receive the information.**

   Note: This provision is unrelated to policy transparency and is not intended to imply that entities not make their face recognition policies available to the public. Rather, this template promotes entity face recognition policy transparency. Refer to Chapter 1. Introduction, Section B. How to Use This Resource, item 3. Transparency and Referencing Other Policies, for guidance on this subject. In addition, refer to section M. Accountability and Enforcement, subsection M.1. Transparency, item 1 within this chapter for the policy provision addressing entity policy transparency.

   The **[name of entity]** will not confirm the existence or nonexistence of face recognition information to any individual or agency that would not be authorized to receive the information unless otherwise required by law.

H. Data Quality Assurance

1. **What is the entity's policy for ensuring that the original image is not altered, changed, or modified?**

   Original probe images will not be altered, changed, or modified in order to protect the integrity of the image. Any enhancements made to a probe image will be made on a copy, saved as a separate image, and documented to indicate what enhancements were made, including the date and time of change.

2. **Does the entity review the quality and suitability of probe images prior to performing a face recognition search?**

   [Name of entity] examiners will analyze, review, and evaluate the quality and suitability of probe images, to include factors such as the angle of the face image, level of detail, illumination, size of the face image, and other factors affecting a probe image prior to performing a face recognition search.

3. **What is the entity's policy regarding use of the face recognition search results for law enforcement action?**

   The **[name of entity]** considers the results, if any, of a face recognition search to be advisory in nature as an investigative lead only. Face recognition search results are **not** considered positive identification of a subject and do not, on their own, establish probable cause, without further investigation. Any possible connection or involvement of the subject(s) to the investigation must be determined through further investigative methods.

   [Add the following statement if the entity utilized mobile face recognition searches.

   All potential matches are considered advisory in nature and any subsequent verification of the individual's identity, such as through a fingerprint check, or follow-on action should be based on an agency's standard operating procedures.]

4. **What is the entity's procedure for ensuring proper face recognition system performance? Routine testing of the face recognition system build, or enhancement, should be performed to ensure the system is operating as designed, continuously available to users without malfunctions or deficiencies, and delivering search results within the accuracy rate of the specific system requirement. Testing also confirms, when system enhancements are made, whether they result in improved performance, (e.g., increased accuracy, speed, filtered search capabilities).**

   The **[name of entity]** will make every reasonable effort to perform routine maintenance, upgrades and enhancements, testing, and refreshes of the face recognition system to ensure proper performance, including the following:
   - Designated, trained personnel shall assess the face recognition system on a regular basis to ensure performance and accuracy.
   - Malfunctions or deficiencies of the system will be reported to the **[insert position/title]** within **[insert time period, e.g., number of days]** of discovering the malfunctions or deficiencies.

5. **Does the entity research alleged errors and malfunctions or deficiencies of face recognition information (or requests that the originating agency or vendor investigates)?**

   The integrity of information depends on quality control and correction of recognized errors which is key to mitigating the potential risk of misidentification or inclusion of individuals in a possible identification. The **[name of entity]** will investigate, in a timely manner, alleged errors and malfunctions or deficiencies of face recognition information or, if applicable, will request that the originating agency or vendor investigate the alleged errors and malfunctions or deficiencies. The **[name of entity]** will correct the information or advise the process for obtaining correction of the information.

I. Disclosure Requests

1. **Does the entity provide face recognition information *to a member of the public* in response to a request based on state open records, sunshine law, or the Freedom of Information Act (FOIA)? For this policy provision, consult with legal counsel to determine under what conditions, if any, face recognition information would be disclosed to a member of the public.**

   Notes:
   - **This issue does not apply to circumstances in which an entity chooses to provide sensitive information in accordance with entity policy in response to an emergency situation or provide nonsensitive information to the public.**
   - **Personal biometric data is generally inaccessible under FOIA. Additional information surrounding face recognition systems and policies may be accessible pursuant to FOIA and state open government laws.**

   Face recognition information will be disclosed to the public in accordance with **[cite applicable state retention laws, public records laws, and policy]**. A record will be kept of all requests and of what information is disclosed to an individual. **[If the state law prohibits disclosure, revise provision to reflect this.]**

J. Redress

J.1 Complaints

1. **What is the entity's procedure for handling individuals' complaints with regard to face recognition information received, maintained, disclosed, or disseminated by the entity?**

   If an individual has a complaint with regard to face recognition information that is exempt from disclosure, is held by the **[name of entity]**, and allegedly has resulted in demonstrable harm to the complainant, the **[name of entity]** will inform the individual of the procedure for submitting (if needed) and resolving such complaints. Complaints will be received by the entity's **[Privacy Officer, Face Recognition Administrator, Internal Affairs Representative, or other position title]** at the following address: **[insert mailing address, e-mail address, and/or link to page if complaints can be submitted electronically]**. The **[Privacy Officer, Face Recognition Administrator, Internal Affairs Representative, or other position title]** will acknowledge the complaint and state that it will be reviewed but will not confirm the existence or nonexistence of the information to the complainant unless otherwise required by law.

   If the face recognition information did not originate with the entity, the **[Privacy Officer, Face Recognition Administrator, Internal Affairs Representative, or other position title]** will notify the originating agency within 30 days in writing or electronically and, upon request, assist such agency to correct any identified data/record deficiencies in the information or verify that the record is accurate.

   All face recognition information held by the entity that is the subject of a complaint will be reviewed within 30 days and confirmed or corrected/purged if determined to be inaccurate or incomplete, to include incorrectly merged or out-of-date information. If there is no resolution within 30 days, the entity will not share the information until such time as the complaint has been resolved. A record will be kept by the entity of all complaints and the resulting action taken in response to them.

J.2 Requests for Corrections

1. **If, in accordance with state statute, the entity is subject to disclosure, what is the entity's procedure for handling individuals' requests for correction involving *face recognition information it can change because it originated the information*? Is a record kept of requests for corrections?**

   If, in accordance with state law, an individual requests correction of face recognition information *originating with the* **[name of entity]** that has been disclosed, the **[name of entity]**'s **[insert title of designee]** will inform the individual of the procedure for requesting a correction. The **[name of entity]** will investigate, in a timely manner, alleged errors and malfunctions or deficiencies of face recognition information or, if applicable, will request that the originating agency or vendor investigate the alleged errors and malfunctions or deficiencies. The **[name of entity]** will correct the information or advise the process for obtaining correction of the information. A record will be kept of all requests and the **[name of entity]**'s response.

J.3 Appeals

1. **If requests for disclosure or corrections are denied, what is the entity's procedure for appeal? Refer to state public records laws and explain the appeals process, including the identity of the office or officer charged with enforcing the public records act; the mailing or e-mail address of the office or officer charged with this responsibility; the time frame for filing the appeal; and the requisite documentation that must be submitted (e.g., a copy of the request, a copy of the response, and a written statement explaining why the requestor asserts that the record is a public record).**

   The individual who has requested disclosure or to whom face recognition information has been disclosed will be informed of the reason(s) why the **[name of entity]** or originating agency denied the request for disclosure or correction. The individual will also be informed of the procedure for appeal when the **[name of entity]** or originating agency has cited an exemption for the type of information requested or has declined to correct challenged face recognition information to the satisfaction of the individual to whom the information relates.

K. Security and Maintenance

1. **What are the entity's physical, procedural, and technical safeguards for ensuring the security and privacy of face recognition information?**

   Describe how the entity will protect the face recognition information from compromise, such as:
   - **Unauthorized access**
   - **Modification**
   - **Theft**
   - **Sabotage (whether internal or external)**
   - **Natural or human-caused disasters**
   - **Intrusions**
   - **Deletion**

   Consider procedures, practices, system protocols, use of software, information technology tools, and physical security measures.

   <u>Best Practice</u>: Reference generally accepted industry or other applicable standard(s) for security with which the entity complies (e.g., National Institute of Standards and Technology guidance).

   The entity will comply with generally accepted industry or other applicable standards for security, in accordance with **[insert the name of the entity security policy or reference applicable standard(s)]** to protect data at rest, in motion, or in use. Security safeguards will cover any type of medium (printed or

electronic) or technology (e.g., physical servers, virtual machines, and mobile devices) used in a work-related **[name of entity]** activity.

The **[name of entity and, if applicable, the name of entity's face recognition vendor]** will operate in a secure facility protected with multiple layers of physical security from external intrusion and will utilize secure internal and external security and privacy safeguards against network intrusions, such as strong multifactor authentication; encrypted communications; firewalls; and other reasonable physical technological, administrative, procedural, and personnel security measures to minimize the risks of unauthorized access to the system. Access to **[name of entity]** face recognition information from outside the facility will be allowed only over secure networks.

All results produced by the [name of entity] as a result of a face recognition search are disseminated by secured electronic means (such as an official government e-mail address). Non-electronic disseminations will be conducted personally or by phone with the requestor or designee.

2. What are the entity's procedures for adhering to data breach notification laws or policies?

All individuals with access to **[name of entity]**'s information or information systems will report a suspected or confirmed breach to the **[Privacy Officer, Face Recognition Administrator, or other position title]** as soon as possible and without unreasonable delay, consistent with applicable laws, regulations, policies, and procedures. This includes a breach in any medium or form, including paper, oral, and electronic.

Best Practice: Provide prompt notification to originating agencies when face recognition information they provided to the entity has been the subject of a suspected or confirmed data breach.

[To the extent allowed by existing data breach notification law] Following assessment of the suspected or confirmed breach and as soon as practicable, the **[name of entity]** will notify the originating agency from which the entity received face recognition information of the nature and scope of a suspected or confirmed breach of such information.

[In addition to the above, the entity should identify any existing laws or policies governing its breach response procedures and, in accordance with these laws and policies, provide specific guidance on breach response procedures, including notification to individuals affected by the breach. Determine whether your state has a data breach notification law and select the appropriate provision.]

Option 1: State, Local, Tribal, or Territorial Data Breach Notification Law

The **[name of entity]** adheres to **[insert citation to applicable data breach notification law.]**. The **[name of entity]** will determine whether a data breach requires notification to an affected individual, in accordance with applicable laws, regulations, policies, and procedures.

Option 2: Office Management and Budget (OMB) Memorandum M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information (January 13, 2017), https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/m-17-12_0.pdf. For additional information on the development of incident response plans, entities may refer to DOJ's *Best Practices for Victim Response and Reporting of Cyber Incidents*, https://www.justice.gov/sites/default/files/opa/speeches/attachments/2015/04/29/criminal_division_guidance_on_best_practices_for_victim_response_and_reporting_cyber_incidents2.pdf.

[Where no applicable state, local, tribal, or territorial law exists, or where entities choose to supplement existing law or policy, M-17-12 may be used as a guide. Entities do not need to adopt OMB M-17-12 in full. Rather, entities should review OMB M-17-12

to determine which provisions are applicable and may adapt those provisions to the specific needs of the entity.]

The **[name of entity]** will adhere to breach procedures established by Office Management and Budget (OMB) Memorandum M-17-12 (January 13, 2017). The provisions adopted by the **[name of entity]** are cited below. In accordance with OMB M-17-12 **[insert citations to the sections and paragraphs of OMB M-17-12 that will be adopted]** and relevant laws, regulations, policies, and procedures, the **[name of entity]** will determine if, when, and how to provide notification to potentially affected individuals and other relevant entities.

Option 3: No State Data Breach Notification Law and Entity Does Not Follow OMB M-17-12

a. Entity Follows an Existing Data Breach Notification Policy

The **[name of entity]** will adhere to the **[name of entity]**'s policy governing data breach notification. In accordance with **[insert citation(s) to the existing policy and procedures]**, the **[name of entity]** will **[insert excerpted language from the policy and procedures, as appropriate here]**. The **[name of entity]** will determine whether a data breach requires notification to an affected individual, in accordance with applicable laws, regulations, policies, and procedures.

b. Entity Does Not Have an Existing Data Breach Notification Policy

[Review and adapt the following template language to reflect the entity's data breach notification policy and procedures.]

When the **[Privacy Officer, Face Recognition Administrator, or other position title]** is notified of a suspected or confirmed breach, the **[Privacy Officer, Face Recognition Administrator, or other position title]** will determine whether the entity's response can be conducted at the staff level or whether a breach response team, consisting of the **[Privacy Officer, Face Recognition Administrator, or other position title, and others (e.g., individual with oversight responsibility for entity operation, the entity security officer, legal counsel, privacy oversight committee, and/or other designee(s))]** must be convened to respond to the breach. The **[Privacy Officer, Face Recognition Administrator, or other position title]**, in coordination with the breach response team, when applicable, will assess the risk of harm to individuals potentially affected by a breach (e.g., the nature and sensitivity of the personally identifiable information [PII] potentially compromised by the breach, the likelihood of access and use of PII, and the type of breach involved), evaluate how the entity may best mitigate the identified risks, and provide recommendations to the **[title of individual with oversight responsibility for entity operation]** on suggested countermeasures, guidance, or other actions.

The **[title of individual with oversight responsibility for entity operation]** will determine whether a data breach requires notification to an affected individual, in accordance with applicable laws, regulations, policies, and procedures. If required, the **[name of entity]** will notify an individual whose PII was or is reasonably believed to have been breached and access to which threatens physical, reputational, or financial harm to that person. If notice to the individual is required, it will be made promptly and without unreasonable delay following discovery of the breach. Notice will be provided consistent with the legitimate needs of law enforcement to investigate the breach or any measures necessary to determine the scope of the breach and, if necessary, to reasonably restore the integrity of any information system affected by the breach.

The **[Privacy Officer, Face Recognition Administrator, or other position title]** is responsible for developing and updating the entity's data breach response plan on an annual basis and in accordance with any changes in law, guidance, standards, agency

policy, procedures, staffing, and/or technology; for maintaining documentation about each data breach reported to the entity and the entity's response; and for keeping entity administrators informed of the status of an ongoing response. The **[title of individual with oversight responsibility for entity operation]** will determine when the response to a breach is concluded, based on input from the **[Privacy Officer, Face Recognition Administrator, or other position title]**.

3. **Is the entity's face recognition system maintained in compliance with the manufacturer's recommendations?**

   All face recognition equipment and face recognition software and components will be properly maintained in accordance with the manufacturer's recommendations, including routine updates as appropriate.

4. **What requirements exist to ensure that the face recognition information will be stored in a secure format and secure environment?**

   The **[name of entity or, if applicable, the name of the entity's face recognition vendor]** will store face recognition information in a manner that ensures that it cannot be modified, accessed, or purged except by personnel authorized to take such actions.

5. **What are the requirements for authorizing personnel to have access to the entity's face recognition system?**

   Authorized access to the **[name of entity]'s** face recognition system will be granted only to personnel whose positions and job duties require such access and who have successfully completed a background check and the training referenced in section N. Training.

6. **Does the entity prohibit sharing of passwords?**

   Usernames and passwords to the face recognition system are not transferrable, must not be shared by **[name of entity]** personnel, and must be kept confidential.

7. **Does the entity require specific configuration of strong passwords and require the replacement of manufacturer default passwords for all web-based system access within a specified time frame?**

   The system administrator will ensure that all manufacturer-generated default passwords are replaced with secure passwords before web-based interfaces of the system become operational. User passwords must meet the following standards **[insert rules, such as no English words and a combination of upper and lowercase letters, numbers, and at least two special characters]**. Authorized users are not permitted to use the same password over time and are required to change their password every **[insert period of time]**.

8. **Does electronic access to the entity's face recognition system identify the user? Is the identity of the user retained in the audit log?**

   Queries made to the **[name of entity]**'s face recognition system will be logged into the system identifying the user initiating the query. All user access, including participating agency access, and queries are subject to review and audit.

9. **Is a log kept of accessed and disseminated entity-owned face recognition information, and is an audit trail maintained? Refer to section M.2. Accountability, for more information on audit logs.**

   The **[name of entity]** will maintain an audit trail of requested, accessed, searched, or disseminated **[name of entity]**-held face recognition information. An audit trail will be kept for a minimum of **[specify the retention period for your jurisdiction/entity for this type of request]** of requests, access, and

searches of face recognition information for specific purposes and of what face recognition information is disseminated to each individual in response to the request.

Audit logs will include:
[Provide a list of the information maintained in the audit log, such as:

- **The name, agency, and contact information of the law enforcement user**
- **The date and time of access**
- **Case number**
- **Probe images (refer to section L.5)**
- **The specific information accessed**
- **The modification or deletion, if any, of the face recognition information**
- **The authorized law enforcement or public safety justification for access (criminal investigation, criminal intelligence, imminent threat, or identification), including a relevant case number if available. Note: The justification should be consistent with section E.]**

L. Information Retention and Purging

Agencies vary on their face recognition image retention policies regarding the specific laws and regulations of their jurisdictions and their strategic and tactical objectives in using the technology. Reference laws, if applicable. If images are stored in multiple repositories (mobile information computer [MDC]/laptops, mobile image capture devices, entity or nonentity servers, etc.), identify each repository and its associated retention period.

1. **What is the entity's retention policy for images contained in the entity's image repository?**

   Notes:

   - **The retention decision focuses on the face recognition record as a whole. Individual components of the face recognition record should not have different retention periods. However, if there are different categories of images that are retained, based on valid law enforcement purposes for retaining the images, include the retention policy for each category of images.**

     For example: "When, in accordance with an official law enforcement activity and this policy, face recognition searches are used for short-term situational awareness surveillance, the [name of entity] will purge face recognition images of nonviolators within [insert time period]. However, with respect to the retention of face recognition images relating to First Amendment-protected events, the [name of entity] limits the retention of face recognition images to [insert time period]."

   - **In accordance with *Recommendations for First Amendment-Protected Events for State and Local Law Enforcement Agencies*,[11] "[a]gencies should limit the retention of information as much as possible to avoid the perception of maintaining files on groups or persons who engage in protected First Amendment activities."**

   [Select all options that are applicable to the entity.]

   Option 1: The entity maintains or operates an entity-owned image repository.

   All images contained within the **[name of entity]**'s **[name of image repository, e.g., mug shot repository]** will be stored for a period not to exceed **[insert a time frame]**. After **[insert time period]**, the information will be automatically purged in accordance with purging

[11] For further information about these processes, see *Recommendations for First Amendment-Protected Events for State and Local Law Enforcement Agencies* at 22–23, Global Justice Information Sharing Initiative, https://it.ojp.gov/GIST/35/Recommendations-for-First-Amendment-Protected-Events-for-State-and-Local-Law-Enforcement-Agencies.

protocols (i.e., permanently removed from the repository). Refer to section K. Security and Maintenance, item 9, regarding face recognition information stored in audit logs.

Option 2: The entity has authorized access to and can perform face recognition searches utilizing image repositories not owned by the entity.

Images accessed by the **[name of entity]** for face recognition searches, in accordance with section E.1, are not maintained or owned by the **[name of entity]** and are subject to the retention policies of the respective agencies authorized to maintain those images.

Option 3: The entity is authorized to request that face recognition searches be performed by an external entity that operates a face recognition program.

The **[name of entity]** is authorized to submit face recognition search requests, in accordance with section E.1, to external agencies that own and maintain face image repositories. The images searched are subject to the retention policies of the respective agencies that maintain or own the face image repositories.

Once a face recognition image is downloaded by **[name of entity]** personnel and incorporated into a criminal intelligence record or an investigative case file, the face recognition information is then considered criminal intelligence or investigative information, and the laws, regulations, and policies applicable to that type of information or criminal intelligence govern its use.

Any images that do not originate with the **[name of entity]** will remain in the custody and control of the originating agency and will not otherwise be transferred to any other entity without authorization from the originating agency.

If the face recognition image has become or there is reason to believe that it will become evidence, including Rosario material or evidence that tends to inculpate or exculpate a suspect, in a specific criminal or other law enforcement investigation or action, the following provisions apply:

a. In those circumstances in which an image is identified as being Rosario material or having evidentiary value, the face recognition **[insert administrator or other title]** or designee will review the facts of the specific case and determine whether the image should be retained beyond the established retention period. If it is determined that it is reasonable to believe the image is Rosario material or has evidentiary value, the face recognition **[insert administrator or other title]** will authorize the transfer of the applicable image from the image repository to **[insert appropriate response; for example, "the entity's investigative case file," "the entity's case management system," or "a form of digital storage media (CD, DVD, etc.) or other portable storage device"]** and will purge the image from the repository.
b. Agencies requiring images be retained by the **[name of entity]** beyond the established retention period may make a formal, written request to the **[name of entity]** to extend retention. Each request must specify the need for extended retention, the circumstances surrounding the request, the requesting agency's case number, and a specific point of contact within the requesting agency. The **[name of entity]** reserves the right to grant or deny agency requests based on the information provided.

The **[name of entity]** retains the right to remove images from the repository earlier than the retention period, based on the limitations of information storage requirements and subject to any applicable record retention laws and statutory disclosure mandates. Early removal, however, will not be used as a means for intentionally interfering with a lawful complaint or a public records request. The retention period may be modified at any time by the **[name of entity]**, subject to applicable legal requirements.

2. **What is the entity's retention policy for probe images?**

   Probe images are not enrolled (stored) in the image repository. Retention of probe images will be the same as for the type of file (criminal case file, criminal intelligence file), whether paper or electronic, in which the information is stored.

3. **Does the entity store unidentified images in an unsolved image file?**

   Note: If the entity does not store images in an unsolved image file, then this provision would not apply. If the entity is going to maintain an unsolved image file, there must be a legal standard and retention period.

   A lawfully obtained probe image of an unknown suspect *may* be added to an unsolved image file pursuant to an authorized criminal investigation. Images in an unsolved image file are periodically compared with those in an image repository (of known persons). If a most likely candidate meets a minimum threshold of computer-evaluated similarity results, the contributor of the probe image is notified and requested to validate the continued need to store the image or determine whether the image can be purged. If, in accordance with this policy, the contributor has not validated the need to retain the image in the unsolved file, the image will be purged.

4. **Does the entity store the results—or generated list of the most likely candidates—of a face recognition search?**

   The list of most likely candidate images is not enrolled (stored) in the image repository. For **[name of entity]** investigations, the case agent will maintain the list of most likely candidates from a face recognition search within the case file.

5. **Are probe images or the results of a face recognition search retained in an audit log?**

   Probe images and face recognition search results are saved within the entity's system audit log for audit purposes only. The audit log is available only to the **[insert position, such as a face recognition administrator]** and will be purged within **[insert time period]**. The audit log is not searchable and face recognition searches cannot be performed using the audit log.

M. Accountability and Enforcement

M.1 Transparency

1. **Is the entity's face recognition policy available to the public?**

   The **[name of entity]** will be open with the public with regard to face recognition information collection, receipt, access, use, dissemination, retention, and purging practices. The **[name of entity]**'s face recognition policy will be made available in printed copy upon request and posted prominently on the **[name of entity]**'s website **[or web page]** at **[insert web address]**.

2. **Does the entity have a point of contact for handling inquiries or complaints?**

   The **[name of entity]**'s **[Privacy Officer, Face Recognition Administrator, or other position title]** will be responsible for receiving and responding to inquiries and complaints about the entity's use of the face recognition system, as well as complaints regarding incorrect information or P/CRCL protections in the image repository maintained and face recognition system accessed by the **[name of entity]**. The **[Privacy Officer, Face Recognition Administrator, or other position title]** may be contacted at **[insert mailing address or e-mail address]**.

M.2 Accountability

1. **What procedures and practices does the entity follow to enable evaluation of user compliance with system requirements, the entity's face recognition policy, and applicable law?**

   The **[name of entity]** will adopt and follow procedures and practices by which it can ensure and evaluate the compliance of users with the face recognition system requirements and with the provisions of this policy and applicable law. This will include logging access to face recognition information, may include any type of medium or technology (e.g., physical servers, virtual machines, and mobile devices) used in a work-related activity, and will entail periodic random auditing of these systems so as not to establish a discernable pattern that may influence users' actions. These audits will be mandated at least **[insert quarterly, semiannually, annually, or other time period]**, and a record of the audits will be maintained by the **[Privacy Officer, Face Recognition Administrator, or title of designee]** of the **[name of entity]** pursuant to the retention policy. Audits may be completed by an independent third party or a designated representative of the **[name of entity]**.

   Appropriate elements of this audit process and key audit outcomes will be compiled into a report and may be provided to command staff and oversight entities or governance boards.[12]

   [Entities may also release a summary of findings to the public, pursuant to law or as a matter of discretion. If so, entities should consider the optional language below.]

   Optional: The **[name of entity]** will provide an overview of audit findings to the public to enhance transparency with respect to P/CRCL protections built into the **[name of entity]**'s operations.

   Note: Statistical data may be incorporated into the publication, but the entity should be mindful of operational considerations. Actual audit logs, statistical data, or summary findings may contain PII. No PII should be included in the summary of audit findings released to the public.

2. **Does the entity have a mechanism for users or other personnel to report errors, malfunctions, or deficiencies of face recognition information and suspected or confirmed violations of face recognition policies?**

   The **[name of entity]**'s personnel or other authorized users shall report errors, malfunctions, or deficiencies of face recognition information and suspected or confirmed violations of the **[name of entity]**'s face recognition policy to the **[name of entity]**'s **[insert title of Face Recognition Administrator]**.

3. **How often does the entity review and update the provisions contained within this face recognition policy (for example, annually)?**

   The **[Privacy Officer, Face Recognition Administrator, or other position title]** will review and update the provisions contained in this face recognition policy annually and will make appropriate changes in response to changes in applicable law, technology, and/or the purpose and use of the face recognition system; the audit review; and public expectations.

[12] *Privacy, Civil Rights, and Civil Liberties Audit Guidance for the State, Local, Tribal, and Territorial Intelligence Component*, Global Justice Information Sharing Initiative, https://it.ojp.gov/GIST/181/Privacy--Civil-Rights--and-Civil-Liberties-Audit-Guidance-for-the-State--Local--Tribal--and-Territorial-Intelligence-Component.

M.3 Enforcement

1. **What is the entity's procedure for enforcement if entity personnel, a participating agency, or an authorized user is suspected of being or has been found to be in noncompliance with the provisions of this policy?**

   If **[name of entity]** personnel, a participating agency, or an authorized user is found to be in noncompliance with the provisions of this policy regarding the collection, receipt, access, use, dissemination, retention, and purging, the **[title of entity director]** of the **[name of entity]** will:
   - Suspend or discontinue access to information by the **[name of entity]** entity personnel, the participating agency, or the authorized user.
   - Apply appropriate disciplinary or administrative actions or sanctions.
   - Refer the matter to appropriate authorities for criminal prosecution, as necessary, to effectuate the purposes of the policy.

2. **What is the entity's policy with regard to the qualifications and number of participating agency personnel authorized to access the entity's face recognition system, and what additional sanctions are available for violations of the entity's face recognition policy?**

   The **[name of entity]** reserves the right to establish the qualifications and number of personnel having access to the **[name of entity]**'s face recognition system and to suspend or withhold service and deny access to any participating agency or participating agency personnel violating this face recognition policy.

N. Training

1. **Which personnel are required to participate in training programs before authorized access to the entity's face recognition system?**

   Before access to the **[name of entity]**'s face recognition system is authorized, the **[name of entity]** will require the following individuals to participate in training regarding implementation of and adherence to this face recognition policy:
   - All authorized **[name of entity]** personnel, including examiners
   - All authorized participating agency personnel
   - All authorized personnel providing information technology services to the **[name of entity]**

2. **What is covered by the entity's face recognition training program (for example, purpose of the face recognition policy, substance and intent of the provisions of the face recognition policy, impact of infractions, and possible penalties for violations)?**

   The **[name of entity]**'s face recognition policy training program will cover both:

   a. Elements of the operation of the face recognition program, including:
      - Purpose and provisions of the face recognition policy.
      - Substance and intent of the provisions of this face recognition policy and any revisions thereto relating to collection, receipt, access, use, dissemination, retention, and purging of the **[name of entity]**'s face recognition information.
      - Policies and procedures that mitigate the risk of profiling.
      - How to implement the face recognition policy in the day-to-day work of the user, whether a paper or systems user.
      - Security awareness training.
      - How to identify, report, and respond to a suspected or confirmed breach.
      - Cultural awareness training, including:

   b. Elements related to the results generated by the face recognition system
      - Originating and participating agency responsibilities and obligations under applicable federal, state, or local law and policy.

- The P/CRCL protections on the use of the technology and the information collected or received, including constitutional protections, and applicable state, local, and federal laws.
- Face recognition system functions, limitations, and interpretation of results.
- Mechanisms for reporting violations of **[name of entity]** face recognition policy provisions.
- The nature and possible penalties for face recognition policy violations, including possible transfer, dismissal, criminal liability, and immunity, if any.

3. **What specialized training does the entity require face recognition examiners to complete prior to performing comparisons and analysis of face recognition probe and candidate images?**

   In addition to the training described in M.2, the **[name of entity]** face recognition examiners are required to complete advanced specialized training to include:
   - Face recognition system functions, limitations, and interpretation of results.
   - Use of image enhancement **[if applicable, "and video editing software"].**
   - Appropriate procedures and how to assess image quality and suitability for face recognition searches.
   - Proper procedures and evaluation criteria for one-to-many and one-to-one face image comparisons.
   - Candidate image verification process.

4. **Does the entity require that investigators (those requesting the entity perform face recognition searches) complete training before they are permitted to make face recognition search requests?**

   Investigators from outside agencies are permitted to request face recognition searches from the **[name of entity]** only if prior to making requests the outside agency **[select applicable entity requirement(s) from the following list or insert the entity's established requirements:**
   - **There is a formalized agreement (e.g., a memorandum of understanding or an interagency agreement) between the [name of entity] and the outside agency, and the agreement acknowledges that requesting investigators have an understanding of the following concepts.**
   - **The outside agency first provides examples of its applicable policies (e.g., privacy) and acknowledges in writing that its requesting investigators have an understanding of the following concepts.**
   - **There is a law enforcement agency that is making the request based on a valid law enforcement purpose that falls within the authorized uses listed in section A. Purpose Statement, item 3. And the requestor provides a case number and contact information (requestor's name, requestor's agency, address, and phone number), and acknowledges an agreement with the following statement:**

     The result of a face recognition search is provided by the [name of entity] only as an investigative lead and IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT. Any possible connection or involvement of any subject to the investigation must be determined through further investigation and investigative resources.

   - **The agency completes the [name of entity]'s training on the following concepts:**
     - **Originating and participating agency responsibilities and obligations under applicable federal, state, or local law and policy.**
     - **P/CRCL protections on the use of the technology and the information collected or received.**
     - **Conditions and criteria under which the face recognition searches may be requested.**
     - **Face recognition system functions, limitations, and interpretation of results.**
     - **Use of face recognition search results as investigative leads only.**
     - **Mechanisms for reporting violations of [name of entity] face recognition policy provisions.**
     - **The nature and possible penalties for face recognition policy violations, including dismissal, criminal liability, and immunity, if any.**
     - **Operational policies.]**

5. What training does the entity require field personnel—who are authorized to run mobile searches—to complete prior to utilizing mobile face recognition search capabilities?

In addition to the training described in N.2, the **[name of entity]** requires all personnel who are authorized to run a mobile search to be trained in the following areas prior to utilizing mobile face recognition search capabilities:

- The proper and lawful use of face images for face recognition purposes.
- How to capture high quality face images in the field for most accurate results.
- The rules and procedures for obtaining an individual's consent to having their image captured.
- The appropriate use and sharing of information obtained from a face recognition search.
- The deletion of field-acquired probe images.

Personnel who have not received this training shall not utilize mobile face recognition search capabilities.

(This Page Intentionally Left Blank)

Appendix A—Glossary of Terms and Definitions

The following is a list of terms and definitions used within the policy or provided for the purpose of enhancing the reader's understanding of the topics discussed.

Access—Information access is being able to get to particular information on a computer (usually requiring permission to use). Web access means having a connection to the internet through an access provider or an online service provider.

Access Control—The mechanisms for limiting access to certain information, based on a user's identity and membership in various predefined groups. Access control can be mandatory, discretionary, or role- or user-based.

Acquisition—The means by which an entity obtains face recognition information through the exercise of its authorities.

Agency—See Participating Agency.

Algorithm—An algorithm is a procedure or formula for solving a problem, based on conducting a sequence of specified actions. A computer program can be viewed as an elaborate algorithm. Algorithms can perform calculation, data processing, and automated reasoning tasks and are widely used throughout all areas of information technology.

Analysis—Refer to Image Analysis.

Attributes—Physical characteristics, such as gender, race, age, hair color, etc. that can be applied to a face recognition search.

Audit Trail—A generic term for recording (logging) a sequence of activities. In computer and network contexts, an audit trail tracks the sequence of activities on a system, such as user log-ins and log-outs. More expansive audit trail mechanisms would record each user's activity in detail, such as what commands were issued to the system, what records and files were accessed or modified, etc.

Audit trails are a fundamental part of computer security and used to trace (albeit usually retrospectively) unauthorized users and uses. They can also be used to assist with information recovery in the event of a system failure.

Authentication—The process of validating the credentials of a person, computer process, or device. Authentication requires that the person, process, or device making the request provides a credential that proves it is what or who it says it is. Common forms of credentials are digital certificates, digital signatures, smart cards, biometrics data, and a combination of user names and passwords. See Biometrics.

Authorization—The process of granting a person, a computer process, or device with access to certain information, services, or functionality. Authorization is derived from the identity of the person, a computer process, or a device requesting access that is verified through authentication. See Authentication.

Automated Face Recognition (AFR)—Automated face recognition (AFR) software compares patterns within the field of computer vision. Such approaches do not rely upon intrinsic models of what a face is, how it should appear, or what it may represent. In other words, the matching is not based on biological or anatomical models of what a face–or the features that make up a face—look like. Instead, the algorithm

performance is entirely dependent upon the patterns which the algorithm developer finds to be most useful for finding similarities. The patterns used in AFR algorithms do not correlate to obvious anatomical features such as the eyes, nose or mouth in a one-to-one manner, although they are affected by these features.

Biometric Template—A biometric template is a set of biometric measurement data [or features] prepared by a face recognition system from a face image.[13] The prepared set can be compared to a probe image. An enrolled image, on its own, is not a biometric template. See Features.

Biometrics—A general term used alternatively to describe (1) a characteristic or (2) a process—(1) a measureable biological (anatomical and physiological) and behavioral characteristic that can be used for automated recognition or (2) automated methods of recognizing an individual based on measureable biological (anatomical and physiological) and behavioral characteristics.[14]

Candidates—See Candidate Images.

Candidate Images—The possible results of a face recognition search. When face recognition software compares a probe image against the images contained in a repository (See Repository.), the result is a list of most likely candidate images that were determined by the software to be sufficiently similar to or most likely resemble the probe image to warrant further analysis. A candidate image is an investigative lead only and does not establish probable cause to obtain an arrest warrant without further investigation.

Candidate List—One or more most likely candidate images resulting from a face recognition search. See Candidate Images.

Center—See Fusion Center.

Civil Liberties—According to the U.S. Department of Justice's Global Justice Information Sharing Initiative, the term "civil liberties" refers to fundamental individual rights, such as freedom of speech, press, or religion; due process of law; and other limitations on the power of the government to restrain or dictate the actions of individuals.[15] They are the freedoms that are guaranteed by the Bill of Rights—the first 10 amendments to the Constitution of the United States. Civil liberties offer protection to individuals from improper government action and arbitrary governmental interference.

Civil Rights—The term "civil rights" refers to those rights and privileges of equal protection that government entities must afford to all individuals in the United States regardless of race, ethnicity, gender, national origin, religion, sexual orientation, gender identity, or other characteristics unrelated to the worth of the individual. Protection of civil rights means that government entities will take action to ensure that individuals are not discriminated against on the basis of any federal- or state- protected characteristic. For example, a state may have constitutional or statutory language regarding parental status. Generally, the term "civil rights" involves positive (or affirmative) government action to protect against infringement, while the term "civil liberties" involves restrictions on government.[16]

Collect—For purposes of this document, "gather" and "collect" mean the same thing.

Comparison—The observation of two or more faces to determine the existence of discrepancies, dissimilarities, or similarities.[17] See Face Comparison.

Computer Security—The protection of information technology assets through the use of technology, processes, and training.

Confidentiality—Refers to the obligations of individuals and institutions to appropriately use information and data under their control once they have been disclosed to them and in accordance with applicable data security laws and policies. See Privacy.

Consent—In general use, consent means compliance in or approval of what is done or proposed by another; specifically, the voluntary agreement or acquiescence by a person of age or with requisite mental capacity who is not under duress or coercion and usually who has knowledge or understanding. Related to mobile face recognition, consent means an individual agrees

[13] Glossary, FISWG, Version 1.1, February 2, 2012, https://www.fiswg.org/FISWG_Glossary_v1.1_2012_02_02.pdf.
[14] Ibid.
[15] *Civil Rights and Civil Liberties Protections Guidance*, at 4 (August 2008), https://www.dni.gov/files/ISE/documents/DocumentLibrary/Privacy/CR-CL_Guidance_08112008.pdf.
[16] The definition of "civil rights" is a modified version of the definition contained in the *National Criminal Intelligence Sharing Plan* (NCISP), at pp. 5–6. *Civil Rights and Civil Liberties Protections Guidance* (August 2008), https://www.dni.gov/files/ISE/documents/DocumentLibrary/Privacy/CR-CL_Guidance_08112008.pdf.
[17] Glossary, FISWG, Version 1.1, February 2, 2012, https://www.fiswg.org/FISWG_Glossary_v1.1_2012_02_02.pdf.

to have his or her image taken by a law enforcement officer for purposes of identification. See Revocation.

Continuous Monitoring—A system security process that comprises ongoing situational awareness of information security, vulnerabilities, threats, and incidents for each user level to support entity risk management decisions.

Credentials—Information that includes identification and proof of identification that are used to gain access to local and network resources. Examples of credentials are usernames, passwords, smart cards, and certificates.

Criminal Activity—A behavior, an action, or an omission that is punishable by criminal law.

Criminal Case Support—Administrative or analytic activities that provide relevant information to law enforcement personnel regarding the investigation of specific criminal activities or trends or specific subject(s) of criminal investigations.

Criminal Intelligence Information—Information deemed relevant to the identification of and the criminal activity engaged in by an individual who or organization that is reasonably suspected of involvement in criminal activity. Criminal intelligence records are maintained in a criminal intelligence system per 28 CFR Part 23.

Data—Inert symbols, signs, descriptions, or measures; elements of information.

Data Breach—The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information (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:

- 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.

Data Protection—Encompasses the range of legal, regulatory, and institutional mechanisms that guide the collection, receipt, use, dissemination, retention, purging, and protection of information.

Data Quality—Refers to various aspects of the information, such as the accuracy and validity of the actual values of the data, information structure, and database/information repository design. Traditionally, the basic elements of data quality have been identified as accuracy, completeness, currency, reliability, and context/meaning. Today, data quality is being more fully described in multidimensional models, expanding conventional views of the topic to include considerations of accessibility, security, and privacy. This concept is also addressed as one of the Fair Information Practice Principles (FIPPs), Data Quality/Integrity. See Appendix B for a full set of FIPPs.

Direct Face Recognition Collection—The entity is owner of the face recognition equipment that captures face recognition information.

Disclosure—The release, transfer, provision of access to, sharing, publication, or divulging of PII in any manner—electronic, verbal, or in writing—to an individual, agency, or organization outside the agency that collected it. Disclosure is an aspect of privacy, focusing on information which may be available only to certain people for certain purposes but which is not available to everyone.

Dissemination—See Disclosure.

Electronically Maintained—Information stored by a computer or on any electronic medium from which the information may be retrieved by a computer, such as electronic memory chips, magnetic tape, magnetic disk, compact disc optical media, or cloud technologies.

Electronically Transmitted—Information exchanged with a computer using electronic media, such as movement of information from one location to another by magnetic or optical media, or transmission over the internet, intranet, extranet, leased lines, dial-up lines, private networks, telephone voice response, or faxback systems. It does not include faxes, telephone calls, video teleconferencing, or messages left on voicemail.

Enhancement—Image enhancement is the process of adjusting digital images so that the results are more suitable for display or further image analysis. For example, removing noise, sharpening or brightening an image may make it easier to identify key features.

Enroll—The process of storing and maintaining information. Specifically in the face recognition context, biometric enrollment is capturing a face image, creating a biometric template from the image, and entering the template into a face recognition repository.[18] See Biometric Template and Repository.

Enrolled Image—An image that is loaded to, and may be stored in, an image repository (see Repository) and used as a reference image for face recognition comparisons (searches). Enrolled images do not include probe images. Some images of individuals may not be enrolled because they do not meet established criteria.

Enrollment—See Enroll.

Entity—The **[name of entity],** which is the subject and owner of the face recognition policy.

Evaluation—Refer to Image Evaluation.

Examiner—An individual who has received advanced training in the face recognition system and its features. Examiners have at least a working knowledge of the limitations of face recognition and the ability to use image editing software. They are qualified to assess image quality and appropriateness for face recognition searches and to perform one-to-many and one-to-one face image comparisons.

Examiners determine if probe images are suitable for face recognition searches, and may enhance images for the purpose of conducting a face recognition search. Though enhancements to the probe image are permissible, the examiner does not base any conclusions on a comparison between an enhanced probe image and a potential candidate photo. Examiners shall evaluate search results by comparing the original unknown probe image with the potential candidate photo.

Expression—Facial aspects resulting from muscle movement or position.[19]

Face Comparison—The manual examination of the differences and similarities between two face images or a live subject and a face image (one-to-one) for the purpose of determining if they represent the same or different persons.[20] See Face Recognition, One-to-One Face Image Comparison, and Verification.

Face Detection—Automated determination of the locations and sizes of human faces in digital images.[21]

Face Examiner—See Examiner.

Face Recognition—The automated searching for a reference image in an image repository (see Repository) by comparing the facial features of a probe image with the features of images contained in an image repository (one-to-many search). A face recognition search will typically result in one or more most likely candidates—or candidate images—ranked by computer-evaluated similarity or will return a negative result. See Candidate Images.

Face Recognition Program—An entity's face recognition initiative that includes the management of human components (management, analysts, examiners, authorized users), ownership and management of the face recognition system (technical components), and the establishment and enforcement of entity-wide processes, policies, and procedures. See Face Recognition System.

Face Recognition Software/Technology—Third-party software that uses specific proprietary algorithms to compare facial features from one specific picture—a probe image—to many others (one-to-many) that are stored in an image repository (see Repository) to determine most likely candidates for further investigation. See Candidate Images.

Face Recognition System—The technical components of a face recognition program, such as hardware, software, interfaces, image repositories, biometric templates, autogenerated candidate lists, etc. While some entities own such a system, others may only have authorized access to another entity's face recognition system. See Face Recognition Program.

Facial Recognition—See Face Recognition.

Fair Information Practice Principles—The Fair Information Practice Principles (FIPPs) are a set of internationally recognized principles that inform information privacy policies both within government and the private sector. Although specific articulations of FIPPs vary and have evolved since their genesis in the 1970s, core elements are consistent among nations, states, and economic sectors. These core elements are incorporated into information privacy

[18] Ibid.
[19] Ibid.
[20] Ibid.
[21] Ibid.

laws, policies, and governance documents around the world. They provide a straightforward description of underlying privacy and information exchange principles and a simple framework for the legal use that needs to be done with regard to privacy in integrated justice systems. Because of operational necessity, it may not always be possible to apply all of the principles equally. For example, the Individual Participation Principle (#8) may be of limited applicability in intelligence operations, as entities do not generally engage with individuals and under federal law, the Privacy Act of 1974 contains exemptions in the law enforcement context. That said, law enforcement entities and all other integrated justice systems should endeavor to apply FIPPs where practicable and ensure compliance with applicable law.

The eight principles are:
1. Purpose Specification
2. Data Quality/Integrity (See definition.)
3. Collection Limitation/Data Minimization
4. Use Limitation
5. Security Safeguards (See definition.)
6. Accountability/Audit
7. Openness/Transparency
8. Individual Participation

See Appendix B for one description of how the U.S. Department of Homeland Security applies these principles.

Features—Observable class or individual characteristics. The components of biometric templates. [22]

Filtering—In the face recognition context, filtering uses relevant physical facial attributes such as eye color, nose shape, eyebrow position, hairline, and other attributes to compare, select, and narrow results. See Attributes.

Firewall—A security solution that segregates one portion of a network from another portion, allowing only authorized network traffic to pass through according to traffic-filtering rules.

Frontal Pose—A face image captured from directly in front of the subject with the focal plane approximately parallel to the plane of the subject's face.[23]

Fusion Center—A fusion center is a collaborative effort of two or more federal, state, local, tribal, or territorial (SLTT) government agencies that combines resources, expertise, or information with the goal of maximizing the ability of such agencies to detect, prevent, investigate, apprehend, and respond to criminal or terrorist activity.[24] State and major urban area fusion centers serve as focal points within the state and local environment for the receipt, analysis, gathering, and sharing of threat-related information between federal and SLTT government agencies and private-sector partners.

Holistic Comparison—The process of comparing faces by looking at the face as a whole and not the component parts in isolation.[25]

Identity—Within a biometric system, the collective set of biographic data, images, and biometric templates assigned to one person.[26] See Face Comparison.

Image—See Probe Image and Repository.

Image Analysis—The assessment of an image to determine suitability for comparison, including the ability to discriminate significant features.[27]

Image Enhancement—See Enhancement.

Image Evaluation—Ascertaining the value of dissimilarities and similarities between two face images, where an examiner assesses the value of the details observed during the analysis and comparison steps and reaches a conclusion.[28]

Image Repository—See Repository.

Individual Characteristics—Characteristics allowing one to differentiate between individuals having the same class of characteristics (e.g., freckles, moles, and scars).[29]

Individual Responsibility—Because a privacy notice is not self-implementing, an individual within an organization's structure must also be assigned responsibility for enacting and implementing the notice.

Individualization—The determination by an examiner that there is sufficient agreement in the quality and quantity of detail to conclude that two

[22] Ibid.
[23] Ibid.
[24] ISE-SAR Functional Standard, version 1.5.5. Source: Section 511 of the 9/11 Commission Act.
[25] Glossary, FISWG, Version 1.1, February 2, 2012, https://www.fiswg.org/FISWG_Glossary_v1.1_2012_02_02.pdf.
[26] Ibid.
[27] Ibid.
[28] Ibid.
[29] Ibid.

images depict the same person.[30] Such results are generally referred for peer and supervisory reviews and approval before any dissemination of results is made.

Information—Includes any data about people, organizations, events, incidents, or objects, regardless of the medium in which it exists. Information received by law enforcement agencies can be categorized into three general areas: general data, including investigative information; tips and leads data, including suspicious activity reports; and criminal intelligence information.

Information Protection—Encompasses the range of legal, regulatory, and institutional mechanisms that guide the collection, receipt, use, dissemination, retention, purging, and protection of information.

Information Quality (IQ)—Refer to Data Quality.

Information Sharing Environment (ISE)—In accordance with Section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended, the Information Sharing Environment (ISE) is a conceptual framework composed of the policies, procedures, and technologies linking the resources (people, systems, databases, and information) of SLTT agencies, federal agencies, and the private sector to facilitate terrorism-related information sharing, access, and collaboration.

Intelligence—See Criminal Intelligence Information.

Invasion of Privacy— Intrusion on an individual's solitude or into an individual's private affairs, public disclosure of embarrassing private information, publicity that puts an individual in a false light to the public, or appropriation of an individual's name or picture for personal or commercial advantage. See also Right to Privacy.

Investigative Lead—Any information which could potentially aid in the successful resolution of an investigation, but does not imply positive identification of a subject or that the subject is guilty of a criminal act.

Known Image—The image of an individual associated with a known or claimed identity and recorded electronically or by other medium (also known as exemplars).[31] Known images are enrolled and stored in an image repository. See Repository.

Law—As used by this policy, law includes any local, state, or federal constitution, statute, ordinance, regulation, executive order, policy, or court rule, decision, or order as construed by appropriate local, state, or federal officials or agencies.

Law Enforcement (LE) Agency—An organizational unit, or subunit, of a local, state, federal, or tribal government with the principal functions of prevention, detection, and investigation of crime, apprehension of alleged offenders, and enforcement of laws. LE agencies further investigations of criminal behavior based on prior identification of specific criminal activity with a statutory ability to perform arrest functions.

Law Enforcement Information—For purposes of the ISE (see Information Sharing Environment), law enforcement information means any information obtained by or of interest to a law enforcement agency or official that is both (a) related to terrorism or the security of our homeland and (b) relevant to a law enforcement mission, including, but not limited to, information pertaining to an actual or potential criminal, civil, or administrative investigation or a foreign intelligence, counterintelligence, or counterterrorism investigation; assessment of or response to criminal threats and vulnerabilities; the existence, organization, capabilities, plans, intentions, vulnerabilities, means, methods, or activities of individuals or groups involved or suspected of involvement in criminal or unlawful conduct or assisting or associated with criminal or unlawful conduct; the existence, identification, detection, prevention, interdiction, or disruption of or response to criminal acts and violations of the law; identification, apprehension, prosecution, release, detention, adjudication, supervision, or rehabilitation of accused persons or criminal offenders; and victim/witness assistance.

Lawful Permanent Resident—A foreign national who has been granted the privilege of permanently living and working in the United States.

Least Privilege Administration—A recommended security practice in which every user is provided with only the minimum privileges needed to accomplish the tasks he or she is authorized to perform.

Logs—A necessary part of an adequate security system which ensures that information is properly tracked and that only authorized individuals are getting access to the data. See also Audit Trail.

Maintenance of Information—Applies to all forms of information storage. This includes electronic systems (for example, databases or repositories) and nonelectronic storage systems (for example, filing

[30] Ibid.

[31] Ibid.

cabinets). To meet access requirements, an organization is not required to create new systems to maintain information or to maintain information beyond a time when it no longer serves an organization's purpose.

Manual Face Examination—Comparison and evaluations of the probe image and the candidate images by a trained biometric images specialist.

Match/Matching—For the purposes of face recognition, see Candidate Images.

Morphological Comparison—The direct comparison of class and individual face characteristics without explicit measurement.[32] See Comparison and Manual Face Examination.

Need to Know—As a result of jurisdictional, organizational, or operational necessities, access to sensitive information or intelligence is necessary for the conduct of an individual's official duties as part of an organization that has a right to know the information to perform or assist in a law enforcement, homeland security, or counterterrorism activity or other lawful and authorized government activity, such as to further an investigation or meet another law enforcement requirement.

Nodal Points—Measurements of distinctive face characteristics, including, but not limited to, the distance between the eyes, width of the nose, and the depth of the eye sockets. Nodal points are extracted from the face image and are transformed through the use of algorithms into a unique file called a biometric template. See Biometric 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 images contained in an image repository.

Non-Criminal Justice Agency—An entity or any subunit thereof that provides services primarily for purposes other than the administration of criminal justice.

One-to-Many 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 most likely candidate images (one-to-many). See Candidate Images.

One-to-One 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 (one-to-one). See Comparison, Face Comparison, and Verification.

Participating Agency—An organizational entity that is authorized to contribute images and/or biometric information to a face recognition system and/or is authorized to access or receive, request, or use face recognition information from the **[name of entity]**'s face recognition system for lawful purposes through its authorized individual users. Participating agencies adhere to conditions defined in a formal agreement (e.g., MOU or interagency agreement) between the **[name of entity]** operating the face recognition program and the participating agency.

Peer Review—An additional layer of verification of face recognition results in a face recognition search process. Examiners submit face recognition search results to other authorized and trained examiners—or peers—for an independent review and cross-verification of the probe and most likely candidate images. If verified by peer(s), this step is generally followed by a supervisor's review and approval prior to dissemination. Refer to Verification.

Permissions—Authorization to perform operations associated with a specific shared resource, such as a file, a directory, or a printer. Permissions must be granted by the system administrator to individual user accounts or administrative groups.

Personally Identifiable Information (PII)—
Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information, that is linked or linkable to a specific individual." [33]

Pose—The orientation of the face with respect to the camera, consisting of pitch, roll, and yaw. Common poses are frontal and profile.[34]

Privacy—Refers to individuals' interests in preventing the inappropriate collection, use, and release of PII. Privacy interests include privacy of personal behavior, privacy of personal communications, and privacy of personal data. Other definitions of privacy include the

[32] Ibid.

[33] For further information about the breadth of PII and how to perform an assessment of the specific risk that an individual can be identified using the information, see Revision of Office of Management and Budget Circular A-130: Managing Information as a Strategic Resource, July 2016, https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/m-17-12_0.pdf.

[34] Ibid.

capacity to be physically left alone (solitude); to be free from physical interference, threat, or unwanted touching (assault, battery); and to avoid being seen or overheard in particular contexts.

Privacy Policy—Short term for a privacy, civil rights, and civil liberties (P/CRCL) policy which is a printed, published statement that articulates the policy position of an organization on how it handles the PII that it gathers or receives and uses in the normal course of business. The policy should include information relating to the processes of information collection, receipt, access, use, dissemination, retention, and purging. It is likely to be informed by the FIPPs. The purpose of the P/CRCL policy is to articulate that the entity will adhere to those legal requirements and entity policy determinations that enable collection, receipt, access, use, dissemination, retention, and purging of information to occur in a manner that protects personal privacy interests. A well-developed P/CRCL policy uses justice entity resources wisely and effectively; protects the entity, the individual, and the public; and promotes public trust.

Probe Image—Any face image used by face recognition software for comparison with the face images contained within a face image repository. See Repository.

A front-facing image of an individual lawfully obtained pursuant to an authorized criminal investigation. Examples of probe images include:

- Face images captured from closed circuit TV cameras
- Face images captured from an ATM camera
- Face images provided by a victim or witness of a crime
- Face images gained from evidence (fraudulent bank card or photograph ID)
- Face sketches (for example, police artist drawings)

Protected Information—For the nonintelligence community, protected information is information about United States citizens and lawful permanent residents that is subject to information privacy or other legal protections under the Constitution and laws of the United States.

For the (federal) intelligence community, protected information includes information about "United States persons" as defined in Executive Order 12333. Protected information may also include other information that the U.S. government expressly determines by Executive Order, international agreement, policy, or other similar instrument.

For state, local, tribal, and territorial governments, protected information may include information about individuals and organizations that is subject to information privacy or other legal protections by law, including the U.S. Constitution; applicable federal statutes and regulations, such as civil rights laws and 28 CFR Part 23; applicable state and tribal constitutions; and applicable state, local, tribal, and territorial laws, ordinances, and codes. Protection may be extended to other individuals and organizations by a law enforcement entity or other state, local, tribal, or territorial agency policy or regulation.

Public—Includes:

- Any individual and any for-profit or nonprofit entity, organization, or association.
- Any governmental entity for which there is no existing specific law authorizing access to the entity's information.
- Media organizations.
- Entities that seek, receive, or disseminate information for whatever reason, regardless of whether it is done with the intent of making a profit and without distinction as to the nature or intent of those requesting information from the entity or participating entity.

Public does not include:

- Any employees of the entity or participating entity.
- People or entities, private or governmental, who assist the entity in the operation of the justice information system.
- Public entities whose authority to access information collected or received and retained by the entity is specified in law.

Public Access—Relates to what information can be seen by the public; that is, information whose availability is not subject to privacy interests or rights.

Purge—A term that is commonly used to describe methods that render data unrecoverable in a storage space or destroy data in a manner that it cannot be reconstituted. There are many different strategies and techniques for data purging, which is often contrasted with data deletion (e.g., made inaccessible except to system administrators or other privileged users).

Recognition—See Face Recognition.

Record—Any item, collection, or grouping of information that includes PII and is collected, received, accessed, used, disseminated, retained, and purged by or for the collecting agency or organization.

Redress—Laws, policies, and procedures that address public agency responsibilities with regard to

access/disclosure and correction of information and the handling of complaints from persons regarding *protected information* about them which is under the entity's control and which is exempt from disclosure and not disclosed to the individual to whom the information pertains.

Protected information includes personal information about individuals that is subject to information privacy or other legal protections by law. Protection may also be extended to organizations by entity policy or state, local, tribal, or territorial law.

Relative Frequency—How often facial features or combinations thereof occur in a given population.[35]

Repository—A location where a group of images of known individuals and biometric templates are stored and managed. An image repository is searched during a face recognition search process whereby a probe image is used by face recognition software for comparison with the images (or features within images) contained in the image repository.

Request—A request received by the **[name of entity]** to utilize face recognition in support of a criminal investigation. Submissions will not contain original evidence. Images received in a request or submission will not be stored as enrolled images within the face recognition system.

Retention—See Storage.

Revocation—In general use, revocation is the act of recall or annulment. It is the reversal of an act, the recalling of a grant or privilege, or the making void of some deed previously existing. As it relates to the revocation of consent to be photographed or the individual's image captured by a law enforcement officer to perform a mobile face recognition search for purposes of identification, once consent to capture an individual's image is given, an individual may withdraw consent with an unequivocal act or statement of withdrawal. Consent may be withdrawn by statements, actions, or a combination of statements and actions. However, the revocation of consent must clearly be a statement revoking consent; an expression of impatience or dislike is not sufficient to terminate consent.

Revoke—See Revocation.

Right to Information Privacy—The right to be left alone, in the absence of some reasonable public interest in collecting, accessing, retaining, and disseminating information about an individual's activities. Invasion of the right to privacy can be the basis for a lawsuit for damages against the individual or entity violating an individual's privacy.

Right to Know—A requirement for access to specific information to perform or assist in a lawful and authorized government function. Right to know is determined by the mission and functions of a law enforcement, homeland security, counterterrorism, or other lawful and authorized government activity, or the roles and responsibilities of particular personnel in the course of their official duties.

Role-Based Access—A type of access authorization that uses roles to determine access rights and privileges. A role is a symbolic category of users that share the same security privilege.

Search—For the purposes of face recognition, the act of comparing a probe image against an image repository.[36] See Repository.

Search Filters—See Filtering.

Search Result Set—The candidate list returned from a face recognition search.[37] See Candidate Images.

Security—Refers to the range of administrative, technical, and physical business practices and mechanisms that aim to preserve privacy and confidentiality by restricting information access to authorized users for authorized purposes. Computer and communications security efforts also have the goal of ensuring the accuracy and timely availability of information for the legitimate user set, as well as promoting failure resistance in the electronic systems overall. Security safeguarding of information is a Fair Information Practice Principle (FIPP). See Appendix B.

Source Entity—Refers to the entity or organizational entity that originates face recognition information.

Storage—In a computer, storage is the place where data is held in electromagnetic or optical form for access by a computer processor. There are two general usages:

- Storage is frequently used to mean the devices and data connected to the computer through input/output operations—that is, hard disk and tape systems and other forms of storage that do not include computer memory and other in-

[35] Glossary, FISWG, Version 1.1, February 2, 2012, https://www.fiswg.org/FISWG_Glossary_v1.1_2012_02_02.pdf.

[36] Ibid.

[37] Ibid.

computer storage. This is probably the most common meaning in the IT industry.

- In more formal usage, storage has been divided into (1) primary storage, which holds data in memory (sometimes called "random access memory," or RAM) and other built-in devices, such as the processor's L1 cache, and (2) secondary storage, which holds data on hard disks, tapes, and other devices requiring input/output operations. Primary storage is much faster to access than secondary storage because of the proximity of the storage to the processor or because of the nature of the storage devices. On the other hand, secondary storage can hold much more data than primary storage.

Submission—See Request.

System Bias—Errors repeatedly introduced through automation (e.g., errors in biometric template generation or comparison). Errors repeatedly introduced through operational practices in an organization or unit (e.g., improper lighting or camera position guidance).[38]

Template—See Biometric Template.

Uncontrolled Image—An image for which the subject did not pose (e.g., security camera images, cell phone photograph taken by a witness).

Unsolved Image File—A lawfully obtained probe image of an unknown suspect *may* be added by authorized law enforcement users to an unsolved image file pursuant to an authorized criminal investigation and if a search has produced no candidates and the subject remains unknown. Images in an unsolved image file are periodically compared with the known images in an image repository. Images enrolled in an unsolved image file should be required to be validated periodically by the contributors to ensure that the criminal investigation remains active and that the image remains relevant to the investigation.

User—An **[name of entity]** employee or an individual representing a participating agency who is authorized and trained to access and use, or receive results from, an entity's face recognition system for lawful purposes.

Valid Law Enforcement Purpose—A purpose for information/intelligence gathering, development, or collection, use, retention, or sharing that furthers the authorized functions and activities of a law enforcement agency, which may include the prevention of crime, ensuring the safety of the public, protection of public or private structures and property, furthering officer safety (including situational awareness), and homeland and national security, while adhering to law and agency policy designed to protect the P/CRCL of Americans.[39] Similar terms include "reasonable law enforcement purpose,"[40] "legitimate law enforcement purpose," and "authorized law enforcement activity."[41]

Verification—In a biometric system, the process of conducting a one-to-one comparison. A task where the face recognition system attempts to confirm an individual's claimed identity by comparing the biometric template generated from a submitted face image with a specific known template generated from a previously enrolled face image.

A review and independent analysis of the conclusion of another examiner.[42]

---

[38] Ibid.

[39] See *Developing a Policy on the Use of Social Media in Intelligence and Investigative Activities: Guidance and Recommendations*, Global, BJA, OJP, DOJ, February 2013, https://it.ojp.gov/GIST/132/Developing-a-Policy-on-the-Use-of-Social-Media-in-Intelligence-and-Investigative-Activities--Guidance-and-Recommendations- and also in the *Real-Time and Open Source Analysis (ROSA) Resource Guide*, Criminal Intelligence Coordinating Council (CICC), Global, BJA, OJP, DOJ, July 2017, https://it.ojp.gov/GIST/1200/Real-Time-and-Open-Source-Analysis--ROSA--Resource-Guide (using "valid law enforcement purpose").

[40] *Recommendations for First Amendment-Protected Events for State and Local Law enforcement Agencies*, CICC, Global, OJP, DOJ, and DHS, December 2011, https://it.ojp.gov/GIST/35/Recommendations-for-First-Amendment-Protected-Events-for-State-and-Local-Law-Enforcement-Agencies.

[41] The term "authorized law enforcement activity" is used, for example, in *The Attorney General's Guidelines For Domestic FBI Operations*, as provided in sections 509, 510, 533, and 534 of title 28, United States Code, and Executive Order 12333, September 29, 2008.

[42] Glossary, FISWG, Version 1.1, February 2, 2012, https://www.fiswg.org/FISWG_Glossary_v1.1_2012_02_02.pdf.

Appendix B—Fair Information Practice Principles (FIPPs)

The Fair Information Practice Principles (FIPPs) are a set of internationally recognized principles that inform information privacy policies within both government and the private sector.

Although specific articulations of FIPPs vary and have evolved since their genesis in the 1970s, core elements are consistent among nations, states, and economic sectors. These core elements are incorporated into data privacy laws, policies, and governance documents around the world. For example, FIPPs are:

- At the core of the Privacy Act of 1974, which applies these principles to U.S. federal agencies.[43]
- Internationally influential, especially as articulated by the Organisation for Economic Co-operation and Development.
- Mirrored in many states' laws and in law enforcement entities' and fusion centers' privacy policies.
- Used by numerous foreign countries and international organizations.

The following formulation of FIPPs is used and implemented for the Information Sharing Environment (ISE) by the U.S. Department of Homeland Security (DHS).[44] For a definition of the Information Sharing Environment, refer to Appendix A, Glossary of Terms and Definitions. Note, however, that under certain circumstances, FIPPs may be superseded by authorities paralleling those provided in the federal Privacy Act; state, local, tribal, or territorial law; or entity policy.

1. **Purpose Specification—**Agencies should specifically articulate the authority that permits the collection of personally identifiable information (PII). The purpose(s) for which PII is collected should be specified at the time of data collection. Subsequent use of this data should be limited to the original purpose for which the PII was collected (or other purposes *compatible* with the original collection purpose).

   Implementing the Purpose Specification Principle—Agencies are bound by specific constitutional and statutory authorities that circumscribe their ability to collect PII. The following are examples of ways agencies may implement this principle:
   - Ensure that a valid lawful purpose exists and is documented for all collection of PII.
   - Include the source and authority for the data so that access restrictions can be applied.
   - Upon receipt of data containing PII from third parties, if possible, identify the purpose for which it was collected initially and limit agency use to only those uses compatible with the original purpose supporting collection.
   - Ensure that metadata or other tags are associated with the data as it is shared.
   - Institute a two-individual review and approval process to consider any Privacy Act or other legal or policy limitation before permitting use or sharing of data for purposes other than that for which it was collected.

[43] 5 U.S.C. § 552a.
[44] 6 U.S.C. § 142.

2. **Data Quality/Integrity—**PII collected should be relevant to the purposes identified for its use and should be accurate, complete, and up to date.

   Implementing the Data Quality/Integrity Principle—One important way to minimize potential downstream privacy and civil liberties concerns is to ensure that any information collected, stored, and disseminated is accurate. This includes ensuring that the information provides sufficient context for any PII. Possible approaches include:
   - Properly labeling PII.
   - Determining a policy for safeguarding PII if there are "mixed" databases (i.e., those databases with personal information on U.S. individuals and others, regardless of nationality).
   - Instituting a source verification procedure to ensure that reporting is based only on authorized data.
   - Reconciling and updating PII whenever new relevant information is collected.
   - Developing a protocol for ensuring that data corrections are passed to those entities with which information has been shared.
   - Creating a documented process for identifying and addressing situations in which data has been erroneously received, is inaccurate, or has been expunged.

3. **Collection Limitation/Data Minimization—**PII should be collected only if the data is directly relevant and necessary to accomplish the specified purpose. PII should be obtained by lawful and fair means and retained only as long as is necessary to fulfill the specified purpose.

   Implementing the Collection Limitation/Data Minimization Principle—Collection limitation may be implemented by:
   - Designing a data storage system to pull data for review and then, if appropriate, automatically purging data after the specified retention period has been reached.
   - Limiting data field elements to only those that are relevant.
   - Ensuring that all distributed reports and products contain only that personal information that is relevant and necessary (nothing extraneous or superfluous).
   - Ensuring that all shared information with PII meets the required thresholds for sharing, such as reasonable suspicion.

4. **Use Limitation—**PII should not be disclosed, made available, or otherwise used for purposes other than those specified except (a) with the consent of the individual or (b) by authority of the law.

   Implementing the Use Limitation Principle—Sharing information should be tempered by adherence to key principles, such as "authorized access." Use limitation may be implemented by:
   - Limiting users of data to those with credential-based access.
   - Requiring that justifications be entered and logs maintained for all queries with sensitive PII and that an internal review process of those logs takes place at specified intervals.
   - Requiring senior analysts to review all reports that use PII before dissemination to ensure (a) that PII is relevant and necessary and (b) that the recipient is authorized to receive the information in the performance of an authorized activity.
   - Prior to sharing information, verify that partners have a lawful purpose for requesting information.
   - Creating multiple use-based distribution lists and restricting distribution to those authorized to receive the information.

5. **Security/Safeguards—**Agencies should institute reasonable security safeguards to protect PII against loss, unauthorized access, destruction, misuse, modification, or disclosure.

   Implementing the Security/Safeguards Principle—This principle can be implemented by:
   - Maintaining up-to-date technology for network security.
   - Ensuring that access to data systems requires that users meet certain training and/or vetting standards and that such access is documented and auditable.
   - Ensuring that physical security measures are in place, such as requiring an identification card, credentials, and/or passcode for data access; disabling computers' USB ports; and implementing firewalls to prevent access to commercial e-mail or messaging services.
   - Implementing a protocol with technical and manual safeguards to ensure the accuracy and completeness of data system purges when records are deleted at the end of their retention period.

- Ensuring that data system purge protocols include complete record deletion on all backup systems.
- Transitioning older repositories into more modern systems to improve access controls.
- Masking data so that it is viewable only to authorized users.
- Maintaining an audit log to record when information is accessed and by whom for review by senior staff at specified intervals.
- Requiring authorized users to sign nondisclosure agreements.

6. **Accountability/Audit—**Agency personnel and contractors are accountable for complying with measures implementing FIPPs, for providing training to all employees and contractors who use PII, and for auditing the actual use and storage of PII.

   Implementing the Accountability/Audit Principle—Strong policies must not only be in place but also be effectively implemented. Accountability can be demonstrated by:
   - Ensuring that upon entry for duty, all staff members take an oath to adhere to the privacy and civil liberties protections articulated in the entity's or host agency's mission, core values statements, other key documents, and/or the U.S. Constitution.
   - Conducting effective orientation and periodic refresher training, including privacy, civil rights, and civil liberties (P/CRCL) protections, for all individuals handling PII.
   - Tailoring training to specific job functions, database access, or data source/storage requirements.
   - Conducting regular audits of all systems in which records are kept to ensure compliance with P/CRCL policies and all legal requirements.
   - Following a privacy incident, establishing a handling procedure for any data breaches or policy violations.
   - Denying database access to individuals until they have completed mandatory systems access training (including training for handling of PII), show a mission need for access, and have any necessary clearances.
   - Developing targeted and consistent corrective actions whenever noncompliance is found.

7. **Openness/Transparency—**To the extent feasible, agencies should be open about developments, practices, and policies with respect to the collection, use, dissemination, and maintenance of PII. Agencies should publish information about policies in this area, including the P/CRCL policy, and contact information for data corrections and complaints.

   Implementing the Openness/Transparency Principle—Agencies can implement the Openness/Transparency principle by:
   - Providing reports to an internal or external oversight body concerned with P/CRCL issues, including P/CRCL audit results.
   - Publishing the P/CRCL policy and redress procedures.
   - Meeting with community groups through initiatives or other opportunities to explain the agency's mission and P/CRCL protections.
   - Responding in the fullest way possible to freedom of information and/or sunshine requests and fully explaining any denial of information requests from the public.
   - Conducting and publishing Privacy Impact Assessments and Privacy Impact Analysis in advance of implementing any new technologies that affect PII, thereby demonstrating that P/CRCL issues have been considered and addressed.

8. **Individual Participation—**To the extent practicable, involve the individual in the process of using PII and seek individual consent for the collection, use, dissemination, and maintenance of PII. Agencies should also provide mechanisms for appropriate access, correction, and redress regarding the agency's use of PII.

   Implementing the Individual Participation Principle—To the extent appropriate, agencies can implement the Individual Participation principle by:
   - Collecting information directly from the individual, to the extent possible and practical.
   - Providing the individual with the ability to find out whether an agency maintains a record relating to him or her and, if not (i.e., access and/or correction is denied), then providing the individual with notice as to why the denial was made and how to challenge such a denial.
   - Putting in place a mechanism by which an individual is able to prevent information about him or her that was obtained for one purpose from being used for other purposes without his or her knowledge.

(This Page Intentionally Left Blank)

Appendix C—Listing of Federal Laws

The U.S. Constitution is known as the primary authority that applies to federal as well as state, local, tribal, and territorial (SLTT) entities. State constitutions cannot provide a lower level of privacy and other civil liberties protection than that established by the U.S. Constitution, but states may broaden constitutional rights guaranteed by their own constitutions.

Civil liberties protections are primarily founded in the Bill of Rights. They include the basic freedoms, such as free speech, assembly, and religion; freedom from unreasonable search and seizure; due process; etc. Statutory civil rights protections in the U.S. Constitution may, in addition, directly govern state action. These include the Civil Rights Act of 1964, as amended; the Rehabilitation Act of 1973; the Equal Educational Opportunities Act of 1974; the Americans with Disabilities Act of 1990; Title VIII of the Civil Rights Act of 1968 (Fair Housing Act); the Voting Rights Act of 1965; and the Civil Rights of Institutionalized Individuals Act.

While in general, SLTT entities may not be bound directly by most statutory federal privacy and other civil liberties protection laws in the face recognition information collection sharing context, compliance may be required **indirectly** by funding conditions (e.g., Title VI of the Civil Rights Act of 1964), operation of the Commerce Clause of the U.S. Constitution, or a binding agreement between a federal agency and an SLTT entity (e.g., a memorandum of agreement or a memorandum of understanding). When relevant or possibly relevant, entities/agencies are advised to list laws, regulations, and policies within their face recognition policies, noting those that may potentially affect the sharing of information.

The development of a face recognition 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 must 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. When staff members know the rules through sound policy and procedure communicated through ongoing training activity, face recognition information sharing is enhanced.

Currently, U.S. federal laws do not specifically address face recognition. A few states have enacted or introduced legislation regarding biometric information. These generally fall into one of three categories regarding the collection, retention, and use of biometric information: (1) of students; (2) by businesses; and (3) by government actors. Three states—Texas,[45] Illinois,[46] and Washington[47]—have adopted laws regulating commercial use of biometric identifiers gathered through certain types of face recognition technology. Five state legislatures (as of

[45] Capture or Use of Biometric Identifier, Texas Business and Commerce Code §503.001.
[46] Biometric Information Privacy Act, 740 Illinois Compiled Statutes 14.
[47] Biometric Identifiers, Washington House Bill 1493, Chapter 299, effective July 23, 2017.

January 1, 2017)—Alaska,[48] Connecticut,[49] Massachusetts,[50] Montana,[51] and New Hampshire[52]—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.[53]

As of February 2011, there is no U.S. federal law requiring that an individual identify him- or herself during a *Terry*[54] stop, but *Hiibel*[55] held that states may enact such laws, provided the law requires the officer to have reasonable and articulable suspicion of criminal involvement.[56] Twenty-four states have enacted stop and identify laws. Although the *Hiibel* case did not directly involve the deputy's use of a 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* and biometric technologies can be addressed through reasonable controls over how face recognition systems are utilized in the field and how the data they capture and create will be managed.[57]

The following are synopses of primary federal laws that an entity should review and, where 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 face recognition 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.

1. **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 nonimmigrant 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 nonimmigrant 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 nonimmigrant status); or (3) aliens who have suffered substantial physical

[48] *Introduced* Collection of Biometric Information, House Bill 72, 2017 Regular Session.
[49] *Introduced* Connecticut House Bill 5522, 2017 Regular Session.
[50] *Introduced* Massachusetts Senate Bill 750, Chapter 93H, Section 1 and 2 2017 Regular Session.
[51] *Introduced* Montana Biometric Information Privacy Act, House Bill 518, 2017 Regular Session.
[52] *Introduced* Biometric Information Privacy Act, New Hampshire House Bill 523, 2017 Regular Session.
[53] *Developing Laws Address Flourishing Commercial Use of Biometric Information,* Claypoole, Ted, and Stoll, Cameron, Business Law Today, American Bar Association, May 2016, https://www.americanbar.org/publications/blt/2016/05/08_claypoole.html.
[54] *Terry v. Ohio*, 392 U.S. 1 (1968).
[55] *Hiibel v. Sixth Judicial District Court*, 542 U.S. 177 (2004).
[56] 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.
[57] *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.

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 nonimmigrant 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 nonimmigrant status, U nonimmigrant status, or relief under VAWA.

2. **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.

3. **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, 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 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.

4. **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 P/CRCL 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 SLTT partners, this tool is useful for identifying and mitigating privacy risks and for notifying the public what PII the SLTT agency is collecting, why PII is being collected, and how the PII will be collected, used, accessed, shared, safeguarded, and stored.

5. **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.

6. **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.[58]

7. **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.

8. **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 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.

9. **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. While state legislatures may pass laws to supplement these federal guidelines, state laws that interfere with or are contrary to a federal law are preempted. 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.

10. **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).

11. **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 except as permitted or required by the rules (45 CFR Part 164.502(a) and §164.103 [defining protected health information 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). Since 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

[58] *Developing Laws Address Flourishing Commercial Use of Biometric Information,* Claypoole, Ted, and Stoll, Cameron, Business Law Today, American Bar Association, May 2016, https://www.americanbar.org/publications/blt/2016/05/08_claypoole.html.

(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. Where a provider determines that such a disclosure is in the patient's best interests, the provider would be permitted to disclose only the protected health information (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 suffering from temporary psychosis or is under the influence of drugs or alcohol.

12. **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.

13. **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 percent of final dispositions be entered in the state databases by December 1998, with steps being taken toward 100 percent 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.

14. **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 that end, SP 800-53 Rev. 4 features eight families of privacy controls that are based on 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.

15. **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.

16. **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*.

17. **Protection of Sensitive Agency Information, Office of Management and Budget Memorandum M-06-16 (June 2006)—**This memorandum provides a security checklist from the National Institute of Standards and Technology (NIST) to protect remote information removed from or accessed from outside an agency's physical location specific to personally identifiable information (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.

18. **REAL ID Act of 2005, Public Law 109–13, Division B, 119 Statute 302, enacted May 11, 2005—**The REAL ID Act requires states to issue driver's licenses and identification cards that comply with standards established by the U.S. Department of Homeland Security if those identifying documents will be used to gain access to federal facilities, board federally regulated commercial aircraft, or enter nuclear power plants. Of particular note, the REAL ID Act requires that a face image be captured for each person ***applying*** for a driver's license or identification card versus existing practices in most states that only capture face images that are ultimately ***issued*** a card. While all states capture face images as part of the routine issuance process for driver's licenses and identification cards, laws in 32 states grant exceptions to the photograph requirement for individuals, including religious objectors, overseas military personnel, and persons unable to visit a service center due to physical disabilities. The REAL ID act further requires departments of motor vehicles to make reasonable efforts to ensure that an applicant does not have more than one driver's license or identification card already issued by that state under a different identity. Many states are already complying with this requirement through the use of face recognition systems. It not only requires the collection of face images but implicitly authorizes the creation of biometric templates used by face recognition systems.

19. **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 Attorney General to bring civil actions to obtain injunctive or declaratory relief to eliminate the unlawful or unconstitutional pattern or practice.

20. **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, speech, 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 D—Sample Face Recognition Policy

The following is a sample face recognition policy that contains all of the sample policy language shown after each question in the template section (Chapter II) of this document. However, while drafting a face recognition policy that includes this language, it is important that the policy author review each question and its associated guidance in the template section while customizing this language. To facilitate this task, the policy language contained in this appendix mirrors the same structure and policy categories as those in the template so that the author can follow each template question, item by item, to customize this language.

It is critical that the policy author not cut and paste the policy language from this appendix (or from the template) and use it as is, without making modifications. There are many areas that prompt the author to insert or customize language. These are shown **bolded and in brackets [ ]**. It is also important to note that this sample policy may not cover all concepts that are unique to your entity's specific face recognition program, and there may be provisions that are not applicable that should be deleted. When developing their policies, law enforcement entities and fusion centers are encouraged to enhance the language with references to applicable statutes, rules, standards, guidelines, and policies.

Finally, since this guidance promotes transparency with the public, each entity should ensure that its policy is written in a manner that is understandable by both entity personnel and members of the public. While some of the provisions in this guidance may reflect concepts and processes long understood and integrated into the daily work of law enforcement such that an entity may not feel they are necessary to be included in its policy, the provisions are included in the sample policy for the purposes of informing the general public and articulating the entity's policies and procedures for P/CRCL throughout the entity face recognition program.

A. Purpose Statement

1. Facial recognition technology involves the ability to examine and compare distinguishing characteristics of a human face through the use of biometric algorithms contained within a software application. This technology can be a valuable investigative tool to detect and prevent criminal activity, reduce an imminent threat to health or safety, and help in the identification of persons unable to identify themselves or deceased persons. The **[name of entity]** has **[implemented or, if applicable, established access and use of]** a face recognition **[program or, if applicable, system]** to support the investigative efforts of law enforcement and public safety agencies both within and outside **[insert state name]**.

2. It is the purpose of this policy to provide **[name of entity]** personnel with guidelines and principles for the collection, access, use, dissemination, retention, and purging of images and related information applicable to the implementation of a face recognition (FR) program. This policy will ensure that all FR uses are consistent with authorized purposes while not violating the privacy, civil rights, and civil liberties (P/CRCL) of individuals.
   Further, this policy will delineate the manner in which requests for face recognition are received, processed, catalogued, and responded to. The Fair Information Practice Principles (FIPPs) form the core of the privacy framework for this policy.

This policy assists **[name of entity]** and its personnel in:

- Increasing public safety and improving state, local, tribal, territorial, and national security.
- Minimizing the threat and risk of injury to specific individuals.
- Minimizing the threat and risk of physical injury or financial liability to law enforcement and others responsible for public protection, safety, or health.
- Minimizing the potential risks to individual privacy, civil rights, civil liberties, and other legally protected interests.
- Protecting the integrity of criminal investigatory, criminal intelligence, and justice system processes and information.
- Minimizing the threat and risk of damage to real or personal property.
- Fostering trust in the government by strengthening transparency, oversight, and accountability.
- Making the most effective use of public resources allocated to public safety entities.

3. All deployments of the face recognition system are for official use only/law enforcement sensitive (FOUO/LES). The provisions of this policy are provided to support the following authorized uses of face recognition information.

[List any of the following that may be applicable and add any other authorized uses that apply to the entity. Note: Uses must be specifically authorized for your entity and must be in accordance with laws, statutes, policies, and procedures governing the entity.

- **A reasonable suspicion that an identifiable individual has committed a criminal offense or is involved in or planning criminal (including terrorist) conduct or activity that presents a threat to any individual, the community, or the nation and that the information is relevant to the criminal conduct or activity.**
- **An active or ongoing criminal or homeland security investigation.**
- **To mitigate an imminent threat to health or safety through short-term situational awareness surveillance or other means.**
- **To assist in the identification of a person who lacks capacity or is otherwise unable to identify him- or herself (such as an incapacitated, deceased, or otherwise at-risk person).**
- **To investigate and/or corroborate tips and leads.**
- **For comparison to determine whether an individual may have obtained one or more official state driver's licenses or identification cards that contain inaccurate, conflicting, or false information.**
- **To assist in the identification of potential witnesses and/or victims of violent crime.**
- **To support law enforcement in critical incident responses and special events.]**

[For those entities using mobile face image capture devices, there may be narrowly tailored purposes for use. Insert the following language and list the purposes that are applicable, and any others that are relevant, to the entity:

Mobile face image searches may be performed only by an officer who has completed training and only during the course of an officer's lawful duties in furtherance of a valid law enforcement purpose and in accordance with the conditions set forth in section F.7 (Refer to F. Use of Face Recognition Information, item 7). Some suggested valid law enforcement purposes include:

- **For persons who are detained for offenses that:**
  - **Warrant arrest or citation or**
  - **Are subject to lawful identification requirements and are lacking positive identification in the field.**
- **For a person who an officer reasonably believes is concealing his or her true identity and has a reasonable suspicion the individual has committed a crime other than concealing his or her identity.**
- **For persons who lack capacity or are otherwise unable to identify him- or herself and who are a danger to themselves or others.**
- **For those who are deceased and not otherwise identified.]**

B. Policy Applicability and Legal Compliance

1. This policy was established to ensure that all images are lawfully obtained, including face recognition probe images obtained or received, accessed, used, disseminated, retained, and purged by the **[name of entity]. This policy also applies to:**
   - Images contained in a known identity face image repository and its related identifying information.
   - **The face image** searching process.
   - Any results from face recognition searches that may be accessed, searched, used, evaluated, retained, disseminated, and purged by the **[name of entity]**.
   - Lawfully obtained probe images of unknown suspects that have been added to unsolved image files (refer to section L.3), pursuant to authorized criminal investigations.

2. All **[name of entity]** personnel, participating agency personnel, and authorized individuals working in direct support of **[name of entity]** personnel (such as interns), personnel providing information technology services to the **[name of entity]**, private contractors, and other authorized users will comply with the **[name of entity]**'s face recognition policy and will be required to complete the training referenced in section N.2. In addition, authorized **[name of entity]** personnel tasked with processing face recognition requests and submissions, must also complete the specialized training referenced in section N.3. An outside agency, or investigators from an outside agency, may request face recognition searches to assist with investigations only if **[insert applicable requirement(s) from those recommended below or insert the entity's established requirements:**
   - **Prior to making requests, the outside agency has a formalized agreement (e.g., a memorandum of understanding or an interagency agreement) between the [name of entity] and the outside agency and the agreement acknowledges that requesting investigators have an understanding of the training concepts listed in section N. Training, item 4.**
   - **The outside agency first provides examples of its applicable policies (e.g., privacy) and acknowledges in writing that its requesting investigators have an understanding of the training concepts listed in section N. Training, item 4.**
   - **The outside agency completes the [name of entity]'s training identified in section N. Training, item 4.**
   - **The outside agency is a law enforcement agency that is making the request based on a valid law enforcement purpose that falls within the authorized uses listed in section A. Purpose Statement, item 3. and the requestor provides a case number and contact information (requestor's name, requestor's agency, address, and phone number) and acknowledges an agreement with the following statement:**

     The result of a face recognition search is provided by the [name of entity] only as an investigative lead and IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT. Any possible connection or involvement of any subject to the investigation must be determined through further investigation and investigative resources.]

3. The **[name of entity]** will provide a printed or electronic copy of this face recognition policy to all:
   - **[name of entity]** and non-**[name of entity]** personnel who provide services
   - Participating agencies
   - Individual authorized users

   The **[name of entity]** will require both a written acknowledgement of receipt of this policy and a written agreement to comply with this policy and its applicable provisions.

4. All **[name of entity]** personnel, participating agency personnel, and authorized individuals working in direct support of **[name of entity]** personnel (such as interns or volunteers), personnel providing information technology services to the **[name of entity]**, private contractors, agencies from which **[name of entity]** information originates, and other authorized users will comply with applicable laws and policies concerning P/CRCL, including, but not limited to **[include a specific reference to any relevant state statutes or other binding state or local policy specific to face recognition systems, then provide**

a list of other applicable state and federal P/CRCL laws and/or include a reference to the section or appendix containing a list of applicable laws].

C. Governance and Oversight

1. Primary responsibility for the operation of the **[name of entity]**'s justice information systems, face recognition program and system, operations, and the coordination of personnel; the receiving, seeking, retention, evaluation, data quality, use, purging, sharing, disclosure, or dissemination of information; and the enforcement of this policy is assigned to the **[position/title]** of the **[name of entity]**.

2. The **[name of entity]**'s **[insert title]** will designate **[a face recognition administrator or face recognition unit or department who/that]** will be responsible for the following **[include any of the following responsibilities that apply to the face recognition administrator or other responsibilities:**
   - **Overseeing and administering the face recognition program to ensure compliance with applicable laws, regulations, standards, and policy.**
   - **Acting as the authorizing official for individual access to face recognition information.**
   - **Ensuring that user accounts and authorities granted to personnel are maintained in a current and secure "need-to-know" status.**
   - **Reviewing face recognition search requests, reviewing the results of face recognition searches, and returning the most likely candidates—or candidate images—if any, to the requesting agency.**
   - **Ensuring that protocols are followed to ensure that face recognition information (including probe images) is automatically purged in accordance with the entity's retention policy (refer to section L.1. Information Retention and Purging), unless determined to be of evidentiary value.**
   - **Ensuring that random evaluations of user compliance with system requirements and the entity's face recognition policy and applicable law are conducted and documented (refer to section M.2. Accountability).**
   - **Confirming, through random audits, that face recognition information is purged in accordance with this policy and to ensure compliance with applicable laws, regulations, standards, and policy.**
   - **Ensuring and documenting that personnel (including investigators from external agencies who may make face recognition search requests) meet all prerequisites stated in this policy prior to being authorized to use the face recognition system.]**

3. **[Select the option that is applicable to the entity.]**

   Option 1: The entity operates its own face recognition program.

   The **[name of entity]** face recognition program was established on **[date]** in conjunction with **[other agency partners, if applicable]**. Personnel from the following agencies are authorized to request face recognition searches:
   - **[Insert list of agencies authorized to request face recognition searches]**.

   Option 2: The entity has authorized access to a face recognition system.

   The **[name of entity]** has authorized access to and can perform face recognition searches utilizing the **[insert name of entity that owns the face recognition program]** face recognition system.

4. The **[name of entity]** contracts with **[insert name of commercial entity or vendor]** to provide **[insert applicable vendor role, such as "software and system development services for the entity's face recognition system"]**. The **[name of entity]** retains ownership of the face recognition system and the images and information it contains.

5. The **[name of entity]** is guided by a **[insert guiding authority, for example, a "designated face recognition oversight committee"]** that ensures that P/CRCL are not violated by this face recognition policy and by the **[name of entity]**'s face recognition information collection, receipt, access, use, dissemination, retention, and purging processes and procedures. The **[insert guiding authority, for example, a "designated face recognition oversight committee"]** engages with the community regarding **[name of entity]'s** face recognition policy prior to publishing.

   It is suggested that the committee will annually review and update the face recognition policy in response to changes in law and program implementation experience, including the results of audits and inspections, and may ***solicit input from the entity's stakeholders*** **[insert, if applicable "and may provide notice to and solicit comment from the public"]** on the development of the face recognition policy or proposed updates to the face recognition policy.

6. The **[insert title of individual or name of entity]** will:
   - Receive reports regarding alleged errors and violations of the provisions of this face recognition policy or applicable state law.
   - Receive and coordinate complaint resolution under the [name of entity]'s face recognition redress policy.
   - Ensure that the provisions of this policy and P/CRCL protections are implemented through efforts such as training, business process changes, and system designs that incorporate privacy-enhancing technologies.

   The **[insert title of individual but not the name or name of entity]** may be contacted at the following address: **[insert phone number, mailing address, or e-mail address]**, which is also posted on **[insert website where this information is listed for purposes of public redress]**.

7. The **[insert title of individual or name of entity]** will ensure that enforcement procedures and sanctions outlined in **[insert section number of policy (see Section M.3. Enforcement)]** are adequate and enforced.

D. Definitions

1. For examples of primary terms and definitions used in this face recognition policy, refer to **[insert section or appendix citation]**.

E. Acquiring and Receiving Face Recognition Information

1. **[Select all options that are applicable to the entity.]**

   Option 1: The entity maintains or operates an entity-owned image repository.

   The **[name of entity]** face recognition system can access and perform face recognition searches utilizing the following entity-owned face image repositories:
   - **[Insert a list of entity-owned and maintained repositories, including information types.]**

   Option 2: The entity has authorized access to and can perform face recognition searches utilizing image repositories not owned by the entity. Indicate the authority/source of the repository (e.g., driver's license photographs).

   The **[name of entity]** is authorized to access and perform face recognition searches utilizing the following external repositories:
   [List the image type and authority/source for each repository accessed. These may include:
   - **Mug-shot images [check state authority and insert source]**

- **Driver's license photographs [check state authority and insert source]**
- **State identification card photographs [check state authority and insert source]**
- **Sex Offender Registry [check state authority and insert source]**
- **[Specify any other image repositories that are accessed and cite state authority.]]**

Option 3: In addition to above, the entity is authorized to request that face recognition searches be performed by an external entity that operates a face recognition program.

In addition to above, the **[name of entity]** is authorized to submit requests for face recognition searches to be performed by the following external entities that own and maintain face image repositories:

[List the image type and authority/source for each repository accessed. These may include:

- **Mug-shot images [check relevant state authority and insert source]**
- **Driver's license photographs [check relevant state authority and insert source]**
- **State identification card photographs [check relevant state authority and insert source]**
- **Sex Offender Registry [check relevant state authority and insert source]**
- **[Specify any other image repositories that are accessed and cite state authority.]]**

2. For the purpose of performing face recognition searches, the **[name of entity]** and authorized **[name of entity]** personnel will obtain probe images or accept probe images from authorized requesting or participating agencies only for the authorized uses identified in section A.2.

3. The **[name of entity]** will receive probe images only from **[list other law enforcement agency or agencies]** in accordance with **[insert mechanisms, e.g., MOU, law, intergovernmental or interagency agreement]** established between the **[name of entity]** and the law enforcement agency(ies). If a non-law enforcement entity wants to submit a probe image for the purpose of a face recognition search, the entity will be required to file a criminal complaint with the appropriate law enforcement entity prior to the search.

4. The **[name of entity]** and, if applicable, any authorized requesting or participating agencies will not violate First, Fourth, and Fourteenth Amendments and will not perform or request face recognition searches about individuals or organizations based solely on their religious, political, or social views or activities; their participation in a particular noncriminal organization or lawful event; or their races, ethnicities, citizenship, places of origin, ages, disabilities, genders, gender identities, sexual orientations, or other classification protected by law.

However, the **[name of entity]** accords special consideration to the collection of face images relating to First Amendment-protected events, activities, and affiliations. Because of the sanctity of the First Amendment, law enforcement's role at First Amendment-protected events is usually limited to crowd control and public safety.[1] If, however, during the planning assessment and approval process for the particular event, before proceeding with the collection, the **[name of entity]** anticipates a need for the collection of face images, the **[name of entity]** will articulate whether collection of face images by law enforcement officers at the event is permissible; the legal or justified basis for such collection (including specifics regarding the criminal behavior that is suspected); and how face images may be collected, used, or retained, in accordance with this policy, as appropriate. If face images will be collected, the plan will specify the type of information collection that is permissible, identify who will collect face images (uniform or plainclothes officers), and define the permissible acts of collection.

[1] For further information about these processes, see *Recommendations for First Amendment-Protected Events for State and Local Law Enforcement Agencies* at 4, Global Justice Information Sharing Initiative, https://it.ojp.gov/GIST/35/Recommendations-for-First-Amendment-Protected-Events-for-State-and-Local-Law-Enforcement-Agencies.

[Note: Some law enforcement purposes may be stated generally in the Operations Plan or communicated to officers, but objectives that may risk interference with the exercise of First Amendment rights should be stated narrowly and be expressly tied to a specific law enforcement function (e.g., public safety, investigative).]

The use of mobile face image capture devices relating to First Amendment-protected events, activities, and affiliations will be specially authorized by **[title of entity supervisor/director/administrator]** of the **[name of entity]** in advance of the event.

The **[name of entity]** will reassess the need for and use of face recognition during the First Amendment-protected event. The **[name of entity]** will utilize face images from a First Amendment-protected event should the public safety mission change or in support of an active or ongoing criminal or homeland security investigation that occurs during or resulted from a First Amendment-protected event.

5. The **[name of entity]** will contract only with commercial face recognition companies or subcontractors that provide assurances that their methods for collecting, receiving, accessing, disseminating, retaining, and purging face recognition information comply with applicable local, state, tribal, territorial, and federal laws, statutes, regulations, and policies and that these methods are not based on unfair or deceptive information collection practices.

F. Use of Face Recognition Information

1. Access to or disclosure of face recognition search results will be provided only ***to individuals within the entity or in other governmental agencies*** who are authorized to have access or have completed applicable training outlined in section N. Training, and only for valid law enforcement purposes (e.g., enforcement, reactive investigations), and to IT personnel charged with the responsibility for system administration and maintenance. Authorized uses are described in A.3 of this policy. [**Insert, if applicable, any additional restrictions or allowances regarding the use of images in briefings or trainings, and whether there are any distinctions for hard-copy versus digital images.]**

2. The **[name of entity]** will prohibit access to and use of the face recognition system, including dissemination of face recognition search results, for the following purposes:
   - Non-law enforcement (including but not limited to personal purposes).
   - Any purpose that violates the U.S. Constitution or laws of the United States, including the protections of the First, Fourth, and Fourteenth Amendments.
   - Prohibiting or deterring lawful individual exercise of other rights, such as freedom of association, implied by and secured by the U.S. Constitution or any other constitutionally protected right or attribute.
   - Harassing and/or intimidating any individual or group.
   - Any other access, use, disclosure, or retention that would violate applicable law, regulation, or policy.

3. The **[name of entity] [does not/does]** connect the face recognition system to any interface that performs live video surveillance, including surveillance cameras, drone footage, and body-worn cameras. The face recognition system **[will not/will]** be configured to conduct face recognition analysis on live or recorded video.

4. The **[name of entity]** will employ credentialed, role-based access criteria, as appropriate, to control:
   - Categories of face recognition information to which a particular group or class of users may have access, based on the group or class.
   - The assignment of roles (e.g., administrator, manager, operator, and user).
   - The categories of face recognition information that a class of users are permitted to access, including information being utilized in specific investigations.
   - Any administrative or functional access required to maintain, control, administer, audit, or otherwise manage the information or equipment.

5. The following describes the **[name of entity]**'s manual and automated face recognition search procedure, which is conducted in accordance with a valid law enforcement purpose and this policy.
   - Authorized **[name of entity]** personnel **[and/or authorized requesting agency personnel]** will submit a probe image of a subject of interest.
   - Trained **[name of entity]** authorized examiners will initially run probe images without filters, using a filtered search as a secondary search, if needed. In some cases, enhancements may be considered after running an image as is against the image repository.
   - In the automated search, most likely candidates are returned to the requestor ranked in order based on the similarity or confidence level.
   - The resulting candidates, if any, are then manually compared with the probe images and examined by an authorized, trained examiner. Examiners shall conduct the comparison of images, biometric identifiers, and biometric information in accordance with their training.
     - If no likely candidates are found, the requesting entity will be informed of the negative results. In the case of a negative result, the images examined by the examiner will not be provided to the requesting entity.
   - Examiners will submit the search and subsequent examination results for a peer review of the probe and candidate images for verification by other authorized, trained examiners.
   - All results of most likely candidate images from the face recognition search must be approved by a supervisor prior to dissemination.
   - All entities receiving the results of a face recognition search must be cautioned that the resulting candidate images do not provide positive identification of any subject, are considered advisory in nature as an investigative lead only, and do not establish probable cause, without further investigation, to obtain an arrest warrant without further investigation.
   - The following statement will accompany the released most likely candidate image(s) and any related records:

     The **[name of entity]** is providing this information as a result of a search, utilizing face recognition software, of records maintained by the **[name of records entity]**. This information is provided only as an investigative lead and **IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT**. Any possible connection or involvement of any subject to the investigation must be determined through further investigation and investigative resources.

6. The **[name of entity]** has established the following process for mobile face recognition searches:
   - Only **[name of entity]** authorized and trained officers may utilize the mobile face recognition application and only on department-authorized devices. **[If personal devices are permitted, insert entity policy regarding use of mobile face recognition on personal devices.]**
   - Prior to utilizing a face recognition search, an officer should first attempt to ascertain an individual's identity by means other than a face recognition search, such as requesting identification, using a fingerprint scanner, etc.
   - Mobile searches may be performed during the course of an officer's lawful duties and only for the entity-established authorized uses listed in section A. Purpose Statement, item 3.
   - In addition, officers may only capture an individual's image when one of the conditions listed in section F.7 exist.
   - **[Use the following language, if the process is applicable to the entity. "The face recognition system does not work over standard cellular internet. Officers must log in and be authenticated into the [name of entity]'s law enforcement network in order to access the face recognition system."]**
   - The log-in screen will prompt the user to acknowledge and agree to the following statement before granting access to the system:
     - Face recognition is not a form of positive identification of a subject. Images returned as a result of a face recognition search may be considered investigative lead information only and are not probable cause to arrest, without further investigation.
     - Face recognition searches shall not be performed by the user on behalf of others who have not been trained and authorized to perform the searches.

- All face recognition searches are subject to audit and require case numbers and file class/crime types.
- Misuse may result in administrative and/or criminal penalties.

- Prior to executing the search, the officer must enter the reason for the search within the application. **[List the reasons that are prompted by the entity's face recognition application. Reasons may include the following:**
  - **Consent**
  - **Reasonable suspicion of a crime**
  - **Probable cause**
  - **Physical/mental incapacity**
  - **Test/training**
  - **Other—[enter written reason]**
- The captured image (probe image) will be submitted to the face recognition system, which will compare the probe image with those contained in the **[indicate the name(s) of repository/ies searched]**.
- A list of most likely candidate images is returned ranked by computer-evaluated similarity.
- The officer then completes a visual or manual morphological comparison of the candidate images with the subject's probe image to make a visual judgment, as well as uses standard investigative techniques, to determine whether the subject is the same as a candidate image.

7. Authorized and trained **[name of entity]** officers may only perform a mobile face recognition search during the course of lawful duties, in accordance with entity-established authorized uses (refer to section A. Purpose Statement, item 3), and when one of the following conditions exist:

- Public Place: In accordance with applicable law, the individual's image is captured in a public place for the purpose of identification and the individual has no reasonable expectation of privacy. The **[name of entity]** will not authorize the collection of the individual's face image when the individual raises an objection that is recognized by law (e.g., religious objection).
- Consent: The individual consents to have his or her image captured for the purpose of identification. The individual may withdraw consent at any time. If consent is withdrawn and neither of the other conditions applies, then use of a face recognition search is not authorized and the search must stop immediately.
- Incapacitation, Defect, or Death: When an individual is unable to provide reliable identification because of physical incapacitation or defect, mental incapacitation or defect, or death, and an immediate identification is needed to assist the officer in the performance of his or her lawful duties.

8. At no time is the use of force permitted to capture a subject's image.

G. Sharing and Disseminating Face Recognition Information

1. The **[name of entity]** will establish requirements for external law enforcement agencies to request face recognition searches. These will be documented in an interagency agreement or MOU, which will include an assurance from the external agency that it complies with the laws and rules governing it, including applicable federal and state laws. The agreement will specify only those agency personnel who have been authorized by the **[name of entity]**, who have completed the required training identified in section N.2, and that requests are for official use only/law enforcement sensitive (FOUO/LES). Each request must be accompanied by a complaint number or case number.

2. The **[name of entity]**'s face recognition search information **will not** be:

- Sold, published, exchanged, or disclosed to commercial or private entities or individuals except as required by applicable law and to the extent authorized by the **[name of entity]**'s agreement with the commercial vendor.
- Disclosed or published without prior notice to the originating entity that such information is subject to disclosure or publication. However, the **[name of entity]** and the originating agency may agree in writing in advance that the **[name of entity]** will disclose face recognition search information as part

of its normal operations, including disclosure to an external auditor of the face recognition search information.
- Disclosed on a discretionary basis unless the originating agency has provided prior written approval or unless such disclosure is otherwise authorized by the MOU or agreement between the **[name of entity]** and the originating agency.
- Disclosed to unauthorized individuals or for unauthorized purposes.
- **[For commercial face recognition vendors, the entity should closely review its vendor agreement.]**

3. The **[name of entity]** will not confirm the existence or nonexistence of face recognition information to any individual or agency that would not be authorized to receive the information unless otherwise required by law.

H. Data Quality Assurance

1. Original probe images will not be altered, changed, or modified in order to protect the integrity of the image. Any enhancements made to a probe image will be made on a copy, saved as a separate image, and documented to indicate what enhancements were made, including the date and time of change.

2. **[Name of entity]** examiners will analyze, review, and evaluate the quality and suitability of probe images, to include factors such as the angle of the face image, level of detail, illumination, size of the face image, and other factors affecting a probe image prior to performing a face recognition search.

3. The **[name of entity]** considers the results, if any, of a face recognition search to be advisory in nature as an investigative lead only. Face recognition search results are **not** considered positive identification of a subject and do not, on their own, establish probable cause, without further investigation. Any possible connection or involvement of the subject(s) to the investigation must be determined through further investigative methods.

   [Add the following statement if the entity utilized mobile face recognition searches.

   All potential matches are considered advisory in nature and any subsequent verification of the individual's identity, such as through a fingerprint check, or follow-on action should be based on an agency's standard operating procedures.]

4. The **[name of entity]** will make every reasonable effort to perform routine maintenance, upgrades and enhancements, testing, and refreshes of the face recognition system to ensure proper performance, including the following:
   - Designated, trained personnel shall assess the face recognition system on a regular basis to ensure performance and accuracy.
   - Malfunctions or deficiencies of the system will be reported to the **[insert position/title]** within **[insert time period, e.g., number of days]** of discovering the malfunctions or deficiencies.

5. The integrity of information depends on quality control and correction of recognized errors which is key to mitigating the potential risk of misidentification or inclusion of individuals in a possible identification. The **[name of entity]** will investigate, in a timely manner, alleged errors and malfunctions or deficiencies of face recognition information or, if applicable, will request that the originating agency or vendor investigate the alleged errors and malfunctions or deficiencies. The **[name of entity]** will correct the information or advise the process for obtaining correction of the information.

I. Disclosure Requests

1. Face recognition information will be disclosed to the public in accordance with **[cite applicable state retention laws, public records laws, and policy]**. A record will be kept of all requests and of what

information is disclosed to an individual. **[If the state law prohibits disclosure, revise provision to reflect this.]**

J. Redress

J.1 Complaints

1. If an individual has a complaint with regard to face recognition information that is exempt from disclosure, is held by the **[name of entity]**, and allegedly has resulted in demonstrable harm to the complainant, the **[name of entity]** will inform the individual of the procedure for submitting (if needed) and resolving such complaints. Complaints will be received by the entity's **[Privacy Officer, Face Recognition Administrator, Internal Affairs Representative, or other position title]** at the following address: **[insert mailing address, e-mail address, and/or link to page if complaints can be submitted electronically]**. The **[Privacy Officer, Face Recognition Administrator, Internal Affairs Representative, or other position title]** will acknowledge the complaint and state that it will be reviewed but will not confirm the existence or nonexistence of the information to the complainant unless otherwise required by law.

   If the face recognition information did not originate with the entity, the **[Privacy Officer, Face Recognition Administrator, Internal Affairs Representative, or other position title]** will notify the originating agency within 30 days in writing or electronically and, upon request, assist such agency to correct any identified data/record deficiencies in the information or verify that the record is accurate.

   All face recognition information held by the entity that is the subject of a complaint will be reviewed within 30 days and confirmed or corrected/purged if determined to be inaccurate or incomplete, to include incorrectly merged or out-of-date information. If there is no resolution within 30 days, the entity will not share the information until such time as the complaint has been resolved. A record will be kept by the entity of all complaints and the resulting action taken in response to them.

J.2 Requests for Corrections

1. If, in accordance with state law, an individual requests correction of face recognition information *originating with the* **[name of entity]** that has been disclosed, the **[name of entity]**'s **[insert title of designee]** will inform the individual of the procedure for requesting a correction. The **[name of entity]** will investigate, in a timely manner, alleged errors and malfunctions or deficiencies of face recognition information or, if applicable, will request that the originating agency or vendor investigate the alleged errors and malfunctions or deficiencies. The **[name of entity]** will correct the information or advise the process for obtaining correction of the information. A record will be kept of all requests and the **[name of entity]**'s response.

J.3 Appeals

1. The individual who has requested disclosure or to whom face recognition information has been disclosed will be informed of the reason(s) why the **[name of entity]** or originating agency denied the request for disclosure or correction. The individual will also be informed of the procedure for appeal when the **[name of entity]** or originating agency has cited an exemption for the type of information requested or has declined to correct challenged face recognition information to the satisfaction of the individual to whom the information relates.

K. Security and Maintenance

1. The entity will comply with generally accepted industry or other applicable standards for security, in accordance with **[insert the name of the entity security policy or reference applicable standard(s)]** to protect data at rest, in motion, or in use. Security safeguards will cover any type of medium (printed or electronic) or technology (e.g., physical servers, virtual machines, and mobile devices) used in a work-related **[name of entity]** activity.

The **[name of entity and, if applicable, the name of entity's face recognition vendor]** will operate in a secure facility protected with multiple layers of physical security from external intrusion and will utilize secure internal and external security and privacy safeguards against network intrusions, such as strong multifactor authentication; encrypted communications; firewalls; and other reasonable physical technological, administrative, procedural, and personnel security measures to minimize the risks of unauthorized access to the system. Access to **[name of entity]** face recognition information from outside the facility will be allowed only over secure networks.

All results produced by the [name of entity] as a result of a face recognition search are disseminated by secured electronic means (such as an official government e-mail address). Non-electronic disseminations will be conducted personally or by phone with the requestor or designee.

2. All individuals with access to **[name of entity]**'s information or information systems will report a suspected or confirmed breach to the **[Privacy Officer, Face Recognition Administrator, or other position title]** as soon as possible and without unreasonable delay, consistent with applicable laws, regulations, policies, and procedures. This includes a breach in any medium or form, including paper, oral, and electronic.

Best Practice Language: [To the extent allowed by existing data breach notification law] Following assessment of the suspected or confirmed breach and as soon as practicable, the **[name of entity]** will notify the originating agency from which the entity received face recognition information of the nature and scope of a suspected or confirmed breach of such information.

[In addition to the above, the entity should identify any existing laws or policies governing its breach response procedures and, in accordance with these laws and policies, provide specific guidance on breach response procedures, including notification to individuals affected by the breach. Determine whether your state has a data breach notification law and select the appropriate provision.]

Option 1: State, Local, Tribal, or Territorial Data Breach Notification Law

The **[name of entity]** adheres to **[insert citation to applicable data breach notification law.]**. The **[name of entity]** will determine whether a data breach requires notification to an affected individual, in accordance with applicable laws, regulations, policies, and procedures.

Option 2: Office Management and Budget (OMB) Memorandum M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information (January 13, 2017), https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/m-17-12_0.pdf. For additional information on the development of incident response plans, entities may refer to DOJ's *Best Practices for Victim Response and Reporting of Cyber Incidents*, https://www.justice.gov/sites/default/files/opa/speeches/attachments/2015/04/29/criminal_division_guidance_on_best_practices_for_victim_response_and_reporting_cyber_incidents2.pdf.

[Where no applicable state, local, tribal, or territorial law exists, or where entities choose to supplement existing law or policy, M-17-12 may be used as a guide. Entities do not need to adopt OMB M-17-12 in full. Rather, entities should review OMB M-17-12 to determine which provisions are applicable and may adapt those provisions to the specific needs of the entity.]

The **[name of entity]** will adhere to breach procedures established by Office Management and Budget (OMB) Memorandum M-17-12 (January 13, 2017). The provisions adopted by the **[name of entity]** are cited below. In accordance with OMB M-17-12 **[insert citations to the sections and paragraphs of OMB M-17-12 that will be adopted]** and relevant laws,

regulations, policies, and procedures, the **[name of entity]** will determine if, when, and how to provide notification to potentially affected individuals and other relevant entities.

Option 3: No State Data Breach Notification Law and Entity Does Not Follow OMB M-17-12

a. Entity Follows an Existing Data Breach Notification Policy

The **[name of entity]** will adhere to the **[name of entity]**'s policy governing data breach notification. In accordance with **[insert citation(s) to the existing policy and procedures]**, the **[name of entity]** will **[insert excerpted language from the policy and procedures, as appropriate here]**. The **[name of entity]** will determine whether a data breach requires notification to an affected individual, in accordance with applicable laws, regulations, policies, and procedures.

b. Entity Does Not Have an Existing Data Breach Notification Policy

[Review and adapt the following template language to reflect the entity's data breach notification policy and procedures.]

When the **[Privacy Officer, Face Recognition Administrator, or other position title]** is notified of a suspected or confirmed breach, the **[Privacy Officer, Face Recognition Administrator, or other position title]** will determine whether the entity's response can be conducted at the staff level or whether a breach response team, consisting of the **[Privacy Officer, Face Recognition Administrator, or other position title, and others (e.g., individual with oversight responsibility for entity operation, the entity security officer, legal counsel, privacy oversight committee, and/or other designee(s))]** must be convened to respond to the breach. The **[Privacy Officer, Face Recognition Administrator, or other position title]**, in coordination with the breach response team, when applicable, will assess the risk of harm to individuals potentially affected by a breach (e.g., the nature and sensitivity of the personally identifiable information [PII] potentially compromised by the breach, the likelihood of access and use of PII, and the type of breach involved), evaluate how the entity may best mitigate the identified risks, and provide recommendations to the **[title of individual with oversight responsibility for entity operation]** on suggested countermeasures, guidance, or other actions.

The **[title of individual with oversight responsibility for entity operation]** will determine whether a data breach requires notification to an affected individual, in accordance with applicable laws, regulations, policies, and procedures. If required, the **[name of entity]** will notify an individual whose PII was or is reasonably believed to have been breached and access to which threatens physical, reputational, or financial harm to that person. If notice to the individual is required, it will be made promptly and without unreasonable delay following discovery of the breach. Notice will be provided consistent with the legitimate needs of law enforcement to investigate the breach or any measures necessary to determine the scope of the breach and, if necessary, to reasonably restore the integrity of any information system affected by the breach.

The **[Privacy Officer, Face Recognition Administrator, or other position title]** is responsible for developing and updating the entity's data breach response plan on an annual basis and in accordance with any changes in law, guidance, standards, agency policy, procedures, staffing, and/or technology; for maintaining documentation about each data breach reported to the entity and the entity's response; and for keeping entity administrators informed of the status of an ongoing response. The **[title of individual with oversight responsibility for entity operation]** will determine when the response to a breach is concluded, based on input from the **[Privacy Officer, Face Recognition Administrator, or other position title]**.

3. All face recognition equipment and face recognition software and components will be properly maintained in accordance with the manufacturer's recommendations, including routine updates as appropriate.

4. The **[name of entity or, if applicable, the name of the entity's face recognition vendor]** will store face recognition information in a manner that ensures that it cannot be modified, accessed, or purged except by personnel authorized to take such actions.

5. Authorized access to the **[name of entity]'s** face recognition system will be granted only to personnel whose positions and job duties require such access and who have successfully completed a background check and the training referenced in section N. Training.

6. Usernames and passwords to the face recognition system are not transferrable, must not be shared by **[name of entity]** personnel, and must be kept confidential.

7. The system administrator will ensure that all manufacturer-generated default passwords are replaced with secure passwords before web-based interfaces of the system become operational. User passwords must meet the following standards **[insert rules, such as no English words and a combination of upper and lowercase letters, numbers, and at least two special characters]**. Authorized users are not permitted to use the same password over time and are required to change their password every **[insert period of time]**.

8. Queries made to the **[name of entity]**'s face recognition system will be logged into the system identifying the user initiating the query. All user access, including participating agency access, and queries are subject to review and audit.

9. The **[name of entity]** will maintain an audit trail of requested, accessed, searched, or disseminated **[name of entity]**-held face recognition information. An audit trail will be kept for a minimum of **[specify the retention period for your jurisdiction/entity for this type of request]** of requests, access, and searches of face recognition information for specific purposes and of what face recognition information is disseminated to each individual in response to the request.

   Audit logs will include:
   [Provide a list of the information maintained in the audit log, such as:
   - **The name, agency, and contact information of the law enforcement user**
   - **The date and time of access**
   - **Case number**
   - **Probe images (refer to section L.5)**
   - **The specific information accessed**
   - **The modification or deletion, if any, of the face recognition information**
   - **The authorized law enforcement or public safety justification for access (criminal investigation, criminal intelligence, imminent threat, or identification), including a relevant case number if available. Note: The justification should be consistent with section E.]**

L. Information Retention and Purging

1. [Select all options that are applicable to the entity.]

Option 1: The entity maintains or operates an entity-owned image repository

All images contained within the **[name of entity]**'s **[name of image repository, e.g., mug shot repository]** will be stored for a period not to exceed **[insert a time frame]**. After **[insert time period]**, the information will be automatically purged in accordance with purging protocols (i.e., permanently removed from the repository). Refer to section K. Security and Maintenance, item 9, regarding face recognition information stored in audit logs.

Option 2: The entity has authorized access to and can perform face recognition searches utilizing image repositories not owned by the entity

Images accessed by the **[name of entity]** for face recognition searches, in accordance with section E.1, are not maintained or owned by the **[name of entity]** and are subject to the retention policies of the respective agencies authorized to maintain those images.

Option 3: The entity is authorized to request that face recognition searches be performed by an external entity that operates a face recognition program.

The **[name of entity]** is authorized to submit face recognition search requests, in accordance with section E.1, to external agencies that own and maintain face image repositories. The images searched are subject to the retention policies of the respective agencies that maintain or own the face image repositories.

Once a face recognition image is downloaded by **[name of entity]** personnel and incorporated into a criminal intelligence record or an investigative case file, the face recognition information is then considered criminal intelligence or investigative information and the laws, regulations, and policies applicable to that type of information or criminal intelligence govern its use.

Any images that do not originate with the **[name of entity]** will remain in the custody and control of the originating agency and will not otherwise be transferred to any other entity without authorization from the originating agency.

If the face recognition image has become or there is reason to believe that it will become evidence, including Rosario material or evidence that tends to inculpate or exculpate a suspect, in a specific criminal or other law enforcement investigation or action, the following provisions apply:

a. In those circumstances in which an image is identified as being Rosario material or having evidentiary value, the face recognition **[insert administrator or other title]** or designee will review the facts of the specific case and determine whether the image should be retained beyond the established retention period. If it is determined that it is reasonable to believe the image is Rosario material or has evidentiary value, the face recognition **[insert administrator or other title]** will authorize the transfer of the applicable image from the image repository to **[insert appropriate response; for example, "the entity's investigative case file," "the entity's case management system," or "a form of digital storage media (CD, DVD, etc.) or other portable storage device"]** and will purge the image from the repository.
b. Agencies requiring images be retained by the **[name of entity]** beyond the established retention period may make a formal, written request to the **[name of entity]** to extend retention. Each request must specify the need for extended retention, the circumstances surrounding the request, the requesting agency's case number, and a specific point of contact within the requesting agency. The **[name of entity]** reserves the right to grant or deny agency requests based on the information provided.

The **[name of entity]** retains the right to remove images from the repository earlier than the retention period, based on the limitations of information storage requirements and subject to any applicable record retention laws and statutory disclosure mandates. Early removal, however, will not be used as a means for intentionally interfering with a lawful complaint or a public records request. The retention period may be modified at any time by the **[name of entity]**, subject to applicable legal requirements.

2. Probe images are not enrolled (stored) in the image repository. Retention of probe images will be the same as for the type of file (criminal case file, criminal intelligence file), whether paper or electronic, in which the information is stored.

3. A lawfully obtained probe image of an unknown suspect *may* be added to an unsolved image file pursuant to an authorized criminal investigation. Images in an unsolved image file are periodically compared with those in an image repository (of known persons). If a most likely candidate meets a minimum threshold of computer-evaluated similarity results, the contributor of the probe image is notified and requested to validate the continued need to store the image or determine whether the image can be purged. Images enrolled in an unsolved image file will be validated on a periodic basis, at least every **[insert time period]**, by the contributors to ensure that the criminal investigation remains active and that the image remains relevant to the investigation. If, in accordance with this policy, the contributor has not validated the need to retain the image in the unsolved file, the image will be purged.

4. The list of most likely candidate images is not enrolled (stored) in the image repository. For **[name of entity]** investigations, the case agent will maintain the list of most likely candidates from a face recognition search within the case file.

5. Probe images and face recognition search results are saved within the entity's system audit log, for audit purposes only. The audit log is available only to the **[insert position, such as a face recognition administrator]** and will be purged within **[insert time period]**. The audit log is not searchable and face recognition searches cannot be performed using the audit log.

M. Accountability and Enforcement

M.1 Transparency

1. The **[name of entity]** will be open with the public with regard to face recognition information collection, receipt, access, use, dissemination, retention, and purging practices. The **[name of entity]**'s face recognition policy will be made available in printed copy upon request and posted prominently on the **[name of entity]**'s website **[or web page]** at **[insert web address]**.

2. The **[name of entity]**'s **[Privacy Officer, Face Recognition Administrator, or other position title]** will be responsible for receiving and responding to inquiries and complaints about the entity's use of the face recognition system, as well as complaints regarding incorrect information or P/CRCL protections in the image repository maintained and face recognition system accessed by the **[name of entity]**. The **[Privacy Officer, Face Recognition Administrator, or other position title]** may be contacted at **[insert mailing address or e-mail address]**.

M.2 Accountability

1. The **[name of entity]** will adopt and follow procedures and practices by which it can ensure and evaluate the compliance of users with the face recognition system requirements and with the provisions of this policy and applicable law. This will include logging access to face recognition information, may include any type of medium or technology (e.g., physical servers, virtual machines, and mobile devices) used in a work-related activity, and will entail periodic random auditing of these systems so as not to establish a discernable pattern that may influence users' actions. These audits will be mandated at least **[insert quarterly, semiannually, annually, or other time period]**, and a record of the audits will be maintained by the **[Privacy Officer, Face Recognition Administrator,**

or title of designee] of the **[name of entity]** pursuant to the retention policy. Audits may be completed by an independent third party or a designated representative of the **[name of entity]**.

Appropriate elements of this audit process and key audit outcomes will be compiled into a report and may be provided to command staff and oversight entities or governance boards.[2]

[Entities may also release a summary of findings to the public, pursuant to law or as a matter of discretion. If so, entities should consider the optional language below.]

Optional: The **[name of entity]** will provide an overview of audit findings to the public to enhance transparency with respect to P/CRCL protections built into the **[name of entity]**'s operations.

Note: Statistical data may be incorporated into the publication, but the entity should be mindful of operational considerations. Actual audit logs, statistical data, or summary findings may contain PII. No PII should be included in the summary of audit findings released to the public.

2. The **[name of entity]**'s personnel or other authorized users shall report errors, malfunctions, or deficiencies of face recognition information and suspected or confirmed violations of the **[name of entity]**'s face recognition policy to the **[name of entity]**'s **[insert title of Face Recognition Administrator]**.

3. The **[Privacy Officer, Face Recognition Administrator, or other position title]** will review and update the provisions contained in this face recognition policy annually and will make appropriate changes in response to changes in applicable law, technology, and/or the purpose and use of the face recognition system; the audit review; and public expectations.

M.3 Enforcement

1. If **[name of entity]** personnel, a participating agency, or an authorized user is found to be in noncompliance with the provisions of this policy regarding the collection, receipt, access, use, dissemination, retention, and purging, the **[title of entity director]** of the **[name of entity]** will:
   - Suspend or discontinue access to information by the **[name of entity]** entity personnel, the participating agency, or the authorized user.
   - Apply appropriate disciplinary or administrative actions or sanctions.
   - Refer the matter to appropriate authorities for criminal prosecution, as necessary, to effectuate the purposes of the policy.

2. The **[name of entity]** reserves the right to establish the qualifications and number of personnel having access to the **[name of entity]**'s face recognition system and to suspend or withhold service and deny access to any participating agency or participating agency personnel violating this face recognition policy.

N. Training

1. Before access to the **[name of entity]**'s face recognition system is authorized, the **[name of entity]** will require the following individuals to participate in training regarding implementation of and adherence to this face recognition policy:
   - All authorized **[name of entity]** personnel, including examiners
   - All authorized participating agency personnel
   - All authorized personnel providing information technology services to the **[name of entity]**

[2] *Privacy, Civil Rights, and Civil Liberties Audit Guidance for the State, Local, Tribal, and Territorial Intelligence Component*, Global Justice Information Sharing Initiative, https://it.ojp.gov/GIST/181/Privacy--Civil-Rights--and-Civil-Liberties-Audit-Guidance-for-the-State--Local--Tribal--and-Territorial-Intelligence-Component.

2. The **[name of entity]**'s face recognition policy training program will cover both:
   a. Elements of the operation of the face recognition program, including:
      - Purpose and provisions of the face recognition policy.
      - Substance and intent of the provisions of this face recognition policy and any revisions thereto relating to collection, receipt, access, use, dissemination, retention, and purging of the **[name of entity]**'s face recognition information.
      - Policies and procedures that mitigate the risk of profiling.
      - How to implement the face recognition policy in the day-to-day work of the user, whether a paper or systems user.
      - Security awareness training.
      - How to identify, report, and respond to a suspected or confirmed breach.
      - Cultural awareness training.
   b. Elements related to the results generated by the face recognition system, including:
      - Originating and participating agency responsibilities and obligations under applicable federal, state, or local law and policy.
      - The P/CRCL protections on the use of the technology and the information collected or received, including constitutional protections, and applicable state, local, and federal laws.
      - Face recognition system functions, limitations, and interpretation of results.
      - Mechanisms for reporting violations of **[name of entity]** face recognition policy provisions.
      - The nature and possible penalties for face recognition policy violations, including possible transfer, dismissal, criminal liability, and immunity, if any.

3. In addition to the training described in M.2, the **[name of entity]** face recognition examiners are required to complete advanced specialized training to include:
   - Face recognition system functions, limitations, and interpretation of results.
   - Use of image enhancement **[if applicable, "and video editing software"].**
   - Appropriate procedures and how to assess image quality and suitability for face recognition searches.
   - Proper procedures and evaluation criteria for one-to-many and one-to-one face image comparisons.
   - Candidate image verification processes.

4. Investigators from outside agencies are permitted to request face recognition searches from the **[name of entity]**, only if prior to making requests the outside agency **[select applicable entity requirement(s) from the following list or insert the entity's established requirements:**
   - **There is a formalized agreement, (e.g., a memorandum of understanding or an interagency agreement), between the [name of entity] and the outside agency and the agreement acknowledges that requesting investigators have an understanding of the following concepts.**
   - **The outside agency first provides examples of its applicable policies (e.g., privacy) and acknowledges in writing that its requesting investigators have an understanding of the following concepts.**
   - **There is a law enforcement agency that is making the request based on a valid law enforcement purpose that falls within the authorized uses listed in section A. Purpose Statement, item 3. And the requestor provides a case number and contact information (requestor's name, requestor's agency, address, and phone number), and acknowledges an agreement with the following statement:**

     The result of a face recognition search is provided by the [name of entity] only as an investigative lead and IS NOT TO BE CONSIDERED A POSITIVEI IDENTIFICATION OF ANY SUBJECT. Any possible connection or involvement of any subject to the investigation must be determined through further investigation and investigative resources.

   - **The agency completes the [name of entity]'s training on the following concepts:**
     - **Originating and participating agency responsibilities and obligations under applicable federal, state, or local law and policy.**
     - **P/CRCL protections on the use of the technology and the information collected or received.**

- **Conditions and criteria under which the face recognition searches may be requested.**
- **Face recognition system functions, limitations, and interpretation of results.**
- **Use of face recognition search results as an investigative lead only.**
- **Mechanisms for reporting violations of [name of entity] face recognition policy provisions.**
- **The nature and possible penalties for face recognition policy violations, including dismissal, criminal liability, and immunity, if any.**
- **Operational policies.]**

5. In addition to the training described in N.2, the **[name of entity]** requires all personnel who are authorized to run a mobile search to be trained in the following areas prior to utilizing mobile face recognition search capabilities:

- The proper and lawful use of face images for face recognition purposes.
- How to capture high quality face images in the field for most accurate results.
- The rules and procedures for obtaining an individual's consent to having their image captured.
- The appropriate use and sharing of information obtained from a face recognition search.
- The deletion of field-acquired probe images.

Personnel who have not received this training shall not utilize mobile face recognition search capabilities.