IDAHO STATE POLICE BUREAU OF CRIMINAL IDENTIFICATION

BIOMETRIC IMAGE COMPARISON (BIC) POLICY FOR CRIMINAL INTELLIGENCE AND INVESTIGATIVE ACTIVITIES

I. Purpose Statement

A. Biometric Image Comparison (BIC) 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 investigate criminal activity and help in the identification of persons unable to identify themselves (incapacitated or deceased persons). The Idaho State Police *Bureau of Criminal Identification (BCI)* has established access to and use of a biometric image comparison system to support the investigative efforts of law enforcement and public safety agencies within Idaho.

B. It is the purpose of this policy to provide Idaho State Police BCI personnel with guidelines and principles for the access, use, dissemination, and purging of images and related information applicable to the implementation of a biometric image comparison program. This policy will ensure that all BIC 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 biometric image comparison are received, processed, responded to, and catalogued. The Fair Information Practice Principles (FIPPs) form the core of the privacy framework for this policy.

   This policy assists the Idaho State Police 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, (P/CRCL) and other legally protected interests.
   - Is minimally intrusive into an individual's P/CRCL.
   - 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.

C. All results of the Biometric image comparison system are to be considered **Law Enforcement Sensitive (LES)** and should only be shared with sworn law enforcement officers or individuals that directly support law enforcement investigations/operations. The provisions of the policy are provided to support the following authorized uses of biometric image comparison information:

a. Reasonable suspicion must exist that an identifiable individual:
   (a) has committed, or is involved in or planning a criminal offense (including terrorism) 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 and the information would be relevant to the investigation or corroboration of case tips/leads or,
   (b) assist a law enforcement agency in the identification of a person who lacks capacity or is otherwise unable to identify him- or herself (such as an incapacitated or deceased person) or,
   (c) In pursuit of a court order.
b. Must be identified to assist with an active criminal case briefing held within a criminal justice agency.
c. Must be identified in the interest of an active or ongoing criminal or homeland security investigation.
d. As part of authorized user training, using only publicly available or volunteer images.

II. Policy Applicability and Legal Compliance

A. This policy has been established to ensure that all images including biometric image comparison probe images, are lawfully obtained, received, accessed, used, disseminated, and purged by the Idaho State Police BCI.
B. This policy also applies to:
   - Images contained in a known identity biometric image repository and corresponding image related Personal Identifying Information (PII).
   - The actual process of biometric image searching.
   - Any results from biometric image comparison searches that may be accessed, searched, used, evaluated, disseminated, and purged by the Idaho State Police.
   - Lawfully obtained probe images of unknown suspects pursuant to documented criminal investigations.
   - Lawfully obtained probe images of unknown incapacitated or deceased individuals pursuant to official identification requests.

B. All Idaho State Police personnel, participating agency personnel, authorized individuals working in direct support of Idaho State Police personnel (such as interns), personnel providing information technology services to the Idaho State Police, private contractors, and other authorized users will comply with the Idaho State Police's biometric image comparison policy and will be required to complete the training referenced in section XIV. Training B. An outside agency, or investigators from an outside agency, may request biometric image comparison searches to assist with investigations only if:
   - 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 I Purpose Statement, item C, and the requestor provides the information outlined in that section and acknowledges an agreement with the following statement:

"The result of a biometric image comparison search is provided by the Idaho State Police 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 Idaho State Police will provide a printed or electronic copy of this biometric image comparison policy to all:
  - Idaho State Police and non-Idaho State Police personnel who provide services
  - Participating agencies that have signed the Idaho Biometric Image Comparison (BIC) Agency Agreement
  - Individual authorized users who have agency approved access to the Idaho BIC program.

  The Idaho State Police will require signatory acknowledgement of receipt of this policy in the form of a signed the Biometric Image Comparison (BIC) Agency Agreement to comply with this policy and its applicable provisions.

- All Idaho State Police personnel, participating agency personnel, authorized individuals working in direct support of Idaho State Police personnel (such as interns or volunteers), personnel providing information technology services to the Idaho State Police, private contractors, agencies from which Idaho State Police information originates, and other authorized users will comply with applicable laws and policies concerning P/CRCL, including but not limited to:
  - Idaho Code Title 67, Chapter 30
  - Federal Bureau of Investigation (FBI) Criminal Justice Information Systems (CJIS) Security Policy (CJISSECPOL)
  - *Public Records Act – Title 74, Chapter 1, Idaho Code*
  - Idaho State Police BIC Usage Policy; ISP Handbook, Chapter 11
  - See Appendix C for additional federal laws

III. Governance and Oversight

A. Primary responsibility for the operation of the Idaho State Police's, biometric image comparison program, operations, and the coordination of personnel; the receiving, seeking, evaluation, data quality, use, purging, sharing, disclosure, or dissemination of information; and the enforcement of this policy is assigned to the Idaho State Police (ISP) Bureau of Criminal identification (BCI).

B. The ISP BCI Chief will designate the Automated Biometric Identification System (ABIS) Technicians who will be responsible for the following:
   - Overseeing and administering the biometric image comparison program to ensure compliance with applicable laws, regulations, standards and policy.
   - Acting as the authorizing official for individual access to biometric image comparison information.
   - Ensuring that user accounts and authorities granted to personnel are maintained in a current and secure "need to know" status.

- Reviewing biometric image comparison search requests, reviewing the results of biometric image comparison searches, and returning the most likely candidates—or candidate images—if any, to the requesting agency.
- Ensuring that protocols are followed to ensure that biometric image comparison submissions (including probe images) are purged in accordance with the Idaho State Police's retention policy as outlined in section XII, A. Information Retention and Purging, unless determined to be of evidentiary value.
- Ensuring that random evaluations of user compliance with system requirements and the Idaho State Police's biometric image comparison policy and applicable law are conducted and documented as outlined in section XIII, B. Accountability.
- Confirming through random audits, that biometric image comparison 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 biometric image comparison search requests) meet all prerequisites stated in this policy prior to being authorized to receive facial image comparison information.

C. The Idaho State Police has authorized access to and can perform biometric image comparison searches utilizing the Federal Bureau of Investigation's (FBI) Interstate Photo System (IPS).

D. The Idaho State Police contracts with the Western Identification Network (WIN) and NEC Corporation of America (NECAM) to provide software and system development services for the Idaho State Police's access to the FBI's Interstate Photo System for purposes of biometric image comparison searches.

E. The Idaho State Police Bureau of Criminal Identification will develop, review, and update BIC policies annually to ensure conformance with P/CRCL requirements.

F. The Idaho State Police Major with authority over Bureau programs will:
   - Receive reports regarding alleged errors and violations of the provisions of this biometric image comparison policy or applicable state law.
   - Receive and coordinate complaint resolution under the Idaho State Police's biometric image comparison 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.

G. The Idaho State Police Major with authority over Bureau programs or the Bureau Chief will ensure that enforcement procedures are adequate and enforced.

IV. Definitions

For examples of primary terms and definitions used in this biometric image comparison policy, see Appendix A at the end of this document.

V. Acquiring and Receiving Biometric Image Comparison Information

A. The Idaho State Police is authorized to access and perform biometric image comparison searches utilizing the following external repositories:
   - The FBI Interstate Photo System [28 CFR §§0.85, 20.31, 20.33; 28 USC §§533, 534; 44 USC §3301; 6 USC §211(g)(4)(C); IdC §67-30]

B. For the purpose of performing biometric image comparison searches, the Idaho State Police and Idaho State Police personnel will obtain probe images or accept probe images from authorized requesting or participating agencies only for the authorized uses identified in section I. 2 of this policy.

C. The Idaho State Police will receive probe images only from Idaho Criminal Justice Agencies in accordance with the Idaho Biometric Image Comparison (BIC) Agency Agreement established between the Idaho State Police and the criminal justice agency(ies). If a non-criminal justice entity needs to submit a probe image for the purpose of a biometric image comparison search, the entity will be required to file a criminal complaint with the appropriate criminal justice agency prior to the search for which the criminal justice agency may submit a probe image based on an active criminal investigation or identification of a person lacking capacity to identify him- or herself.

D. The Idaho State Police and, if applicable, any authorized requesting or participating agencies will not violate the First, Fourth, and Fourteenth Amendments of the United States Constitution and or Article 1 of the Idaho Constitution) and will not perform or request biometric image comparison 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.

VI. Use of Biometric Image Comparison Information

A. Access to, or disclosure of biometric image comparison 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 or agreements as outlined in this policy and only for valid criminal justice purposes as outlined in section I. C of this policy.

B. The Idaho State Police will <u>prohibit access</u> to and use of the biometric image comparison system, including dissemination of biometric image comparison search results, for the following purposes:

   - Non-criminal justice (including but not limited to personal purposes).

- Any purpose that violates the constitution of the state of Idaho and 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.

C. The Idaho State Police does not connect the biometric image comparison system to any interface that performs live video surveillance, including surveillance cameras, drone footage, and body-worn cameras. The biometric image comparison system will not be configured to extract biometric images from live or recorded video.
    a. Still shots from live or recorded video, extracted by the submitting agency for comparison, will be accepted.

D. The Idaho State Police will employ credentialed, role-based access criteria, as appropriate, to control:

- Categories of biometric image comparison 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 biometric image comparison 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.

E. The following describes the Idaho State Police's manual and automated biometric image comparison search procedure, which is conducted in accordance with a valid criminal justice purpose and this policy.

- Authorized Idaho State Police personnel and/or authorized requesting agency personnel will submit a probe image of a subject of interest.
- Trained Idaho State Police authorized Biometric Examiners will initially run probe images without filters, using a filtered search (using investigative data to refine a search and improve search results) as a secondary search, if needed. In some cases, enhancements (typically minor in nature: contrast/brightness/gamma correction or "mirroring" the visible portion of a face) 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 Biometric 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 biometric image comparison search must be approved by a supervisor prior to dissemination.
- All image dissemination should be done as a Law Enforcement Sensitive (LES) product and only recipients outlined above should receive such.
- **All entities receiving the results of a biometric image comparison 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 Idaho State Police is providing this information as a result of a search, utilizing biometric image comparison software, of records maintained by the Federal Bureau of Investigation. 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.*

VII. Sharing and Disseminating Biometric Image Comparison Information

A. The Idaho State Police will establish requirements for external law enforcement agencies to request biometric image comparison searches. These will be documented in an interagency agreement, 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 Idaho State Police, who have completed the required training identified in section XIV. D, and that requests are Law Enforcement Sensitive (LES). Each request must be accompanied by a complaint, incident, or case number.

B. The Idaho State Police's biometric image comparison search information **will not** be:

- Sold, published, exchanged, or disclosed to commercial or private entities or individuals except as required by applicable law including, but not limited to Title 74, Chapter 1, Idaho Code.
- Disclosed or published without prior notice to the originating entity that such information is subject to disclosure or publication.
- 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 Idaho State Police and the originating agency.

- Disclosed to unauthorized individuals or for unauthorized purposes.

C. The Idaho State Police will not confirm the existence or nonexistence of biometric image comparison information to any individual or agency that would not be authorized to receive the information unless otherwise required by law.

VIII. Data Quality Assurance

A. 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.

B. Idaho State Police 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 biometric image comparison search.

C. The Idaho State Police considers the results, if any, of a biometric image comparison search to be advisory in nature as an investigative lead only. Biometric image comparison 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.

D. Routine testing of the biometric image comparison processes will be performed as part of the overall biometric comparison system to ensure it 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. Verification across populations will also be included to ensure the system remediates any unintended bias.

E. The integrity of information depends on quality control and correction of recognized errors, mitigating the potential risk of misidentification or inclusion of individuals in a possible identification. The Idaho State Police ABIS vendor will investigate any errors or malfunctions within the WIN system. The Idaho State Police ABIS vendor will assist in remediating external database search issues as necessary.

IX. Disclosure Requests

Biometric image comparison information will only be disclosed to the extent required by Title 74, Chapter 1, Idaho Code or other applicable law.

X. Redress

X.1 Complaints

A. If an individual has a complaint with regard to biometric image comparison information that is exempt from disclosure, is held by the Idaho State Police, and allegedly has resulted in demonstrable harm to the complainant, the Idaho State Police will inform the individual of the procedure for submitting (if needed), and resolving, such complaints. Complaints will be received by the Idaho State Police Major with authority over Bureau programs at the following address: 700 S. Stratford Dr., Meridian, Idaho 83642. The ISP Major 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 biometric image comparison information did not originate with the Idaho State Police, the ISP Major 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.

X.2 Requests for Corrections

A. If, in accordance with state law, an individual requests correction of biometric image comparison information *originating with the FBI* that has been disclosed, the Idaho State Police will inform the individual of the procedure for requesting a correction. The Idaho State Police will notify the FBI, in a timely manner, of any alleged errors and malfunctions or deficiencies in the mechanism accessing the biometric image comparison repository at the FBI, and will request that the FBI investigate the alleged incorrect information. The Idaho State Police will advise the individual on the process for obtaining correction of the information. A record will be kept of all requests and the Idaho State Police's response.

X.3 Appeals

A. If the challenged record was originated by another agency, the individual shall contact the originating agency and follow the process for requesting correction and appealing denial of a request for correction as applicable by law to that originating agency's records.

B. If the challenged record originated from the Idaho State Police, applicable procedures depend by law upon the nature of the particular record: Idaho Code Title 67, Chapter 30, Idaho Code Title 74, Chapter 1, IDAPA 11.10.02 – Rules Governing State Criminal History Records and Crime Information, or other potentially applicable law pertain to different types of records. C. Upon determination of the type of record, the Idaho State Police will notify the individual of the applicable process available to the individual.

XI. Security and Maintenance

A. The Idaho State Police will comply with applicable standards for security, in accordance with the FBI Criminal Justice Information Services (CJIS) Security Policy, U.S. Code of Federal Regulations, National Institute of Standards and Technology (NIST) guidelines and Idaho state law 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, etc.) used in a work-related Idaho State Police biometric image comparison activity.

The Idaho State Police and its partners, WIN and NECAM, will operate in secure facilities 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 Idaho State Police's biometric image comparison information from outside the facility will be allowed only over secure networks.

All results produced by the Idaho State Police as a result of a biometric image comparison search are disseminated by secured electronic means. Non-electronic disseminations will be conducted personally or by phone with the requestor or designee.

B. All individuals with access to Idaho State Police's biometric image comparison information or information systems will report a suspected or confirmed breach to the ISP Information Security Officer (ISO) 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.

C. Notifying originating agency

To the extent not prohibited by Title 28, Chapter 51, Idaho Code, or other applicable law, following assessment of the suspected or confirmed breach and as soon as practicable, the Idaho State Police will notify the originating agency from which the entity received biometric information of the nature and scope of a suspected or confirmed breach of such information.

The Idaho State Police follows the Idaho Technology Authority (ITA) Cybersecurity Incident and Breach Response Reporting procedures which can be found on the ITA website (https://ita.idaho.gov/resources/), ITA Guidelines, G585.

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

E. The Idaho State Police and WIN/NECAM will store biometric image comparison search information in a manner that ensures that it cannot be modified, accessed, or purged except by personnel authorized to take such actions.

F. Authorized access to the Idaho State Police's biometric image search system will be granted only to personnel whose positions and job duties require such access and who have successfully completed a fingerprint-based background check and the training referenced in section XIV. Training.

G. Usernames and passwords to the biometric image comparison system are not transferrable, must not be shared by Idaho State Police personnel, and must be kept confidential.

H. 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 basic standard as identified in the FBI CJIS Security Policy current version. Authorized users are not permitted to use the same password over time and are required to change their password every 90 days.

I. Queries made to the Idaho State Police's biometric image comparison system will be logged by the system identifying the user initiating the query. All user access, including participating agency access, and queries are subject to review and audit.

J. The Idaho State Police's biometric image comparison system, managed and maintained by NECAM will maintain an audit trail of requested, accessed, and searched, FBI Interstate Photo System-held biometric image comparison information. An audit trail of requests and searches of biometric image comparison information for specific purposes will be kept indefinitely. The Idaho State Police will maintain an audit trail for system access and dissemination of biometric image comparison search results for specific purposes and of what biometric image comparison information is disseminated to each individual in response to the request.

System audit logs will include:

- The username of the Idaho State Police personnel accessing the system
- Agency ORI and contact information from the requesting agency personnel submitting the request for a biometric image comparison search
- The date and time of access
- Originating Agency Case number
- The modification or deletion, if any, of the biometric image comparison information disseminated

The Idaho State Police will maintain audit information on:

- The authorized criminal justice justification for access (criminal investigation or identification of a deceased person)

XII. Information Retention and Purging

A. Images accessed by the Idaho State Police for biometric image comparison searches, in accordance with section V. A, are not maintained or owned by the Idaho State Police and are subject to the retention policies of the respective agencies authorized to maintain those images.

Once a probe image is submitted for system comparison by Idaho State Police personnel and incorporated into an authorized law enforcement agency's criminal intelligence record or an investigative case file, the biometric comparison 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 probe images that do not originate with the Idaho State Police 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.

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

C. The list of most likely candidate images is not enrolled (stored) in any image repository.

D. Biometric image comparison search results are saved within the Idaho State Police's ABIS system vendor audit log for audit purposes only. The audit log is available only to system administrators and will be retained indefinitely.

XIII. Accountability and Enforcement

XIII 1. Transparency

A. The Idaho State Police will be open with the public with regard to biometric image comparison information collection, receipt, access, use, dissemination, retention, and purging practices. The Idaho State Police's biometric image comparison policy will be made available in printed copy upon request and posted prominently on the Idaho State Police's website at https://isp.idaho.gov/bci/criminal-history/.

B. The Idaho State Police's Major with authority over BCI programs, will be responsible for receiving and responding to inquiries and complaints about the entity's use of the biometric image comparison system, as well as complaints regarding incorrect information or P/CRCL protections in the image repository maintained and biometric image comparison system accessed by the Idaho State Police. The ISP Major with authority over BCI programs may be contacted at 700 S. Stratford Dr., Meridian, ID, 83642.

XIII 2. Accountability

A. The Idaho State Police will adopt and follow procedures and practices by which it can ensure and evaluate the compliance of users with the biometric image comparison system requirements and with the provisions of this policy and applicable law. This will include logging access to biometric image comparison information, may include any type of medium or technology (e.g., physical servers, virtual machines, etc.) 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 annually, and a record of the audits will be maintained by the Major with authority over BCI programs of the Idaho State Police pursuant to the retention policy. Audits may

be completed by an independent third party or a designated representative of the Idaho State Police.

B. The Idaho State Police's personnel or other authorized users shall report errors, malfunctions, or deficiencies of biometric image comparison information and suspected or confirmed violations of the Idaho State Police's biometric image comparison policy to the Idaho State Police's Major with authority over BCI programs.

C. The ISP Major with authority over BCI programs will review and update the provisions contained in this biometric image comparison policy annually and will make appropriate changes in response to changes in applicable law, technology, and/or the purpose and use of the biometric image comparison system; the audit review; and public expectations.

XIII 3. Enforcement

A. If Idaho State Police 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 Director of the Idaho State Police may:

- Suspend or discontinue access to information by the Idaho State Police entity personnel, the participating agency, or the authorized user.
- Apply other disciplinary or administrative actions or sanctions.
- Refer the matter to appropriate authorities for criminal prosecution, as necessary, to effectuate the purposes of the policy.

B. The Idaho State Police reserves the right to establish the qualifications and number of personnel having access to the Idaho State Police's biometric image comparison system and to suspend or withhold service and deny access to any participating agency or participating agency personnel violating this biometric image comparison policy.

XIV. Policy Training

A. Before access to the Idaho State Police's biometric image comparison system is authorized, the Idaho State Police will require the following individuals to participate in training regarding implementation of and adherence to the biometric image comparison policy:

- All participating authorized Idaho State Police personnel, including examiners
- All participating authorized participating agency personnel
- All participating authorized personnel providing information technology services to the Idaho State Police, with physical or logical access to the BIC software

B. The Idaho State Police's biometric image comparison policy training program will cover:

- Elements of the operation of the biometric image comparison program including:
    - Purpose and provision of the biometric image comparison policy.
    - Substance and intent of the provision of this biometric image comparison policy and any revisions thereto relating to collection, receipt, access, use, dissemination, retention, and purging of the Idaho State Police's biometric image comparison information.
    - Policies and procedures that mitigate the risk of profiling.
    - How to implement the biometric image comparison 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
- Elements related to the results generated by the biometric image comparison 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.
    - Biometric image comparison system functions, limitations, and interpretation of results.
    - Mechanisms for reporting violations of Idaho State Police biometric image comparison policy provisions.
    - The nature and possible penalties for biometric image comparison policy violations, including possible transfer, dismissal, criminal liability, and immunity, if any.

C. In addition to the training described in the previous section, the Idaho State Police biometric image comparison examiners are required to complete advanced specialized training to include:
    - biometric image comparison system functions, limitations, and interpretation of results.
    - Use of basic image enhancement functionality (contrast, brightness, etc.) that is part of the software. No specialty or third-party applications or software will be available in the system.
    - Appropriate procedures and how to assess image quality and suitability for biometric image comparison searches.
    - Proper procedures and evaluation criteria for one-to-many and one-to-one biometric image comparisons.
    - Candidate image verification process.

D. Investigators from outside agencies are permitted to request biometric image comparison searches from the Idaho State Police only if prior to making requests:
    - There is a criminal justice agency that is making the request based on a valid law enforcement purpose that falls within the authorized uses listed in section I. Purpose

Statement, section C. 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 biometric image comparison search is provided by the Idaho State Police only as an investigative lead and IS NOT TO BE CONSIDERED A POSTIVE IDENTIFICATION OF ANY SUBJECT. Any possible connection or involvement of any subject to the investigation must be determined through further investigation and investigative resources.

- There is a formalized agreement between the Idaho State Police and the outside agency, and the agreement acknowledges that requesting investigators have an understanding of 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 biometric image comparison searches may be requested.
    - Biometric image comparison system functions, limitations, and interpretation of results.
    - Use of biometric image comparison search results as investigative leads only.
    - Mechanisms for reporting violations of Idaho State Police biometric image comparison policy provisions.
    - The nature and possible penalties for biometric image comparison policy violations, including dismissal, criminal liability, and immunity, if any.

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 biometric comparison information through the exercise of its authorities.

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.

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 Biometric Image Comparison (ABIC)—Automated biometric image comparison (ABIC) 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 ABIC 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.

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 comparison or (2) automated methods of recognizing an individual based on measureable biological (anatomical and physiological) and behavioral characteristics.[1]

Candidate Images—The possible results of a biometric image comparison search. When biometric image comparison 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 biometric image comparison search. See Candidate Images.

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 ofindividuals.[2] 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.[3]

Comparison—The observation of two or more candidate images to determine the existence of discrepancies, dissimilarities, or similarities of the probe image.[4] See **Biometric Image** 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.

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

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.

Criminal Justice Agency-- (1) Courts; and (2) A governmental agency or any subunit thereof that performs the administration of criminal justice pursuant to a statute or executive order, and that allocates a substantial part of its annual budget to the administration of criminal justice. See Law Enforcement Agency.

Data Breach—"Breach of the security of the system" means the illegal acquisition of unencrypted computerized data that materially compromises the security, confidentiality, or integrity of personal information for one (1) or more persons maintained by an agency, individual or a commercial entity. Good faith acquisition of personal information by an employee or agent of an agency, individual or a commercial entity for the purposes of the agency, individual or the commercial entity is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

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.

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.

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 biometric image comparisons (searches). Enrolled images do not include probe images. Some images of individuals may not be enrolled because they do not meet established criteria.

Entity—The Idaho State Police, which is the subject and owner of the biometric image comparison policy.

Examiner—An individual who has received advanced training in the biometric image comparison system and its features. Examiners have at least a working knowledge of the limitations of biometric image comparison and the ability to use image editing software. They are qualified to assess image quality and appropriateness for biometric image comparison searches and to perform one-to-many and one-to-one biometric image image comparisons.
Examiners determine if probe images are suitable for biometric image comparison searches, and may enhance images for the purpose of conducting a biometric image comparison 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.

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

Biometric Image Examiner—See Examiner.

Biometric Image Comparison—The automated searching for a reference image in an image repository (see Repository) by comparing the biometric image features of a probe image with the features of images contained in an image repository (one-to-many search). A biometric image comparison 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.

Biometric Image Comparison Program—An entity's biometric image comparison initiative that includes the management of human components (management, analysts, examiners, authorized users), ownership and management of the biometric image comparison system (technical components), and the establishment and enforcement of entity-wide processes, policies, and procedures.

Biometric Image Comparison Software/Technology—Third party software that uses specific proprietary algorithms to compare biometric image 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.

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 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.

Filtering—In the biometric image comparison context, filtering uses relevant physical biometric attributes such as eye color, nose shape, eyebrow position, hairline, and other attributes to compare, select, and narrow results.

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 biometric image captured from directly in front of the subject with the focal plane approximately parallel to the plane of the subject's face.[5]

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.

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.

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. See Criminal Justice Agency.

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.

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.

One-to-Many Biometric 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 [6] in a list of most likely candidate images (one-to-many). See Candidate Images.

One-to-One Biometric 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, **Biometric Image** Comparison, and Verification.

Participating Agency—An organizational entity that is authorized to access or receive, request, or use biometric image comparison information from the Idaho State Police's biometric image comparison 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 Idaho State Police operating the biometric image comparison program and the participating agency.

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." [7]

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.

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 biometric image used by biometric image comparison software for comparison with the biometric images

contained within a biometric image repository. See Repository.

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

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

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.

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).

Record—Any item, collection, or grouping of information that includes PII and is collected, received, accessed, used, disseminated, retained, or 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.

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 biometric image comparison search process whereby a probe image is used by biometric image comparison software for comparison with the images (or features within images) contained in the image repository.

Request—A request received by the Idaho State Police to utilize biometric image comparison in support of a criminal investigation or to identify a deceased person of interest to an authorized participating agency. Submissions will not contain original evidence. Images received in a request or submission will not be stored as enrolled images within the biometric image comparison system.

Search—For the purposes of biometric image comparison, the act of comparing a probe image against an image repository.[8] See Repository.

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.

User—An Idaho State Police employee or an individual representing a participating agency who is authorized and trained to access and use, or receive results from, an entity's biometric comparison 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.[9] Similar terms include "reasonable law enforcement purpose,"[10] "legitimate law enforcement purpose," and "authorized law enforcement activity."[11]

Verification—In a biometric system, the process of conducting a one-to-one comparison. A task where the biometric image comparison system attempts to confirm an individual's claimed identity by comparing the biometric template generated from a submitted biometric image with a specific known template generated from a previously enrolled biometric image. A review and independent analysis of the conclusion of another examiner.[12]

Footnotes:

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

[2]*Civil Rights and Civil Liberties Protections Guidance*, at4 (August 2008), https://www.dni.gov/files/ISE/documents/DocumentLibrary/Privacy/CR-CL_Guidance_08112008.pdf.

[3]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.

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

[5]Ibid.

[6]Ibid.

[7]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.

[8]Ibid.

[9]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-onthe- 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").

[10]*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.

[11]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.

[12]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.

1. **Purpose Specification—** It is the purpose of this policy to provide Idaho State Police BCI personnel and authorized agency users with guidelines and principles for the access, use, dissemination, and purging of images and related information applicable to the implementation of a biometric image comparison (FIC) program. This policy will ensure that all FIC 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 biometric image comparison 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 the Idaho State Police, its personnel, and authorized users 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.

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.

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.

---

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

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 biometric image comparison 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).

This biometric image comparison 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.

Currently, U.S. federal laws do not specifically address biometric image comparison. 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.

Finally, many state laws governing data security and breach response include biometric information in their definitions of covered personal information.

As biometric image comparison information may be incorporated as one piece of information into a larger case file, the following federal laws may be applicable.

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**

2. **Criminal Intelligence Systems Operating Policies, 28 CFR Part 23, Code of Federal Regulations, Title 28, Chapter 1, Part 23**

3. **Driver's Privacy Protection Act (DPPA) of 1994, 18 U.S.C. 2721 and 2725**

4. **E-Government Act of 2002, Public Law 107– 347, 208, 116 Stat. 2899 (2002**)

5. **Enhanced Border Security and Visa Reform Act of 2002, H.R. 3525**

6. **Federal Civil Rights laws, 42 U.S.C. § 1983, United States Code, Title 42, Chapter 21, Subchapter I, § 1983**

7. **Indian Civil Rights Act of 1968, 25 U.S.C. § 1301 et seq., United States Code, Title 25, Chapter 15, Subchapter I**

8. **National Child Protection Act of 1993, Public Law 103-209 (December 20, 1993), 107 Stat. 2490**

9. **NIST Special Publication 800-53 (Appendix J)** ***Security and Privacy Controls for Federal Information Systems and Organizations***

10. **Privacy Act of 1974, 5 U.S.C. § 552a, United States Code, Title 5, Part I, Chapter 5, Subchapter II, § 552a**

11. **Protection of Sensitive Agency Information, Office of Management and Budget Memorandum M-06-16 (June 2006)**

12. **Section 210401 of the Violent Crime Control and Law Enforcement Act of 1994, 42 U.S.C. § 14141**

13. **U.S. Constitution, First, Fourth, Fifth, Sixth, and Fourteenth Amendments**