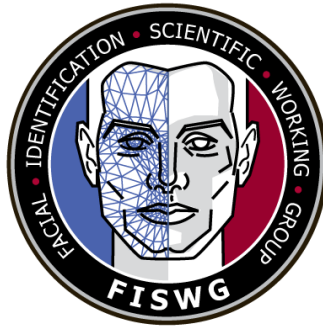




Disclaimer:

As a condition to the use of this document and the information contained herein, the Facial Identification Scientific Working Group (FISWG) requests notification by email before or contemporaneously to the introduction of this document, or any portion thereof, as a marked exhibit offered for or moved into evidence in any judicial, administrative, legislative, or adjudicatory hearing or other proceeding (including discovery proceedings) in the United States or any foreign country. Such notification shall include: 1) the formal name of the proceeding, including docket number or similar identifier; 2) the name and location of the body conducting the hearing or proceeding; and 3) the name, mailing address (if available) and contact information of the party offering or moving the document into evidence. Subsequent to the use of this document in a formal proceeding, it is requested that FISWG be notified as to its use and the outcome of the proceeding. Notifications should be sent to: chair@fiswg.org

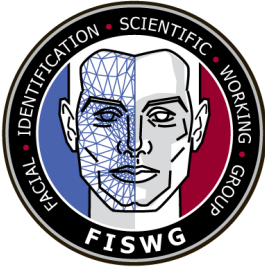
Redistribution Policy:

FISWG grants permission for redistribution and use of all publicly posted documents created by FISWG, provided that the following conditions are met:

Redistributions of documents, or parts of documents, must retain the FISWG cover page containing the disclaimer.

Neither the name of FISWG, nor the names of its contributors, may be used to endorse or promote products derived from its documents.

Any reference or quote from a FISWG document must include the version number (or creation date) of the document and mention if the document is in a draft status.



Recommendations for Defensible Facial Recognition Technology Use

1. Scope

1.1 This document translates evolving legal expectations, governance frameworks, and operational practices into structured recommendations intended to be implemented as a coherent set broken down in three separate areas:

1.1.1 Legal readiness and disclosure

1.1.2 Operational assurance and auditability

1.1.3 Public transparency and engagement

1.2 These recommendations are intended to help agencies ensure that the use of Facial Recognition Technology (FRT) can be clearly documented, explained, and evaluated when relied upon in investigative or evidentiary contexts, including potential court proceedings. Where appropriate, recommendations are aligned with Facial Identification Scientific Working Group (FISWG) Responsible Use Principles, the Facial Recognition Technology Implementation Guidelines, and the Operational Assurance document series.

2. Referenced Documents

2.1 *FISWG Standards:*

Principles for Responsible Use of Facial Recognition Technology

Facial Recognition Technology Implementation Guidelines

Facial Recognition Systems Operation Assurance

Glossary and Acronyms

3. Terminology

3.1 *Definitions:*

3.1.1 Terminology should, where appropriate, reflect definitions and usage set out in the FISWG Glossary, the Responsible Use Principles, the Facial Recognition Technology Implementation Guidelines, and the Operational Assurance document series.

4. Summary of Practice

4.1 Public trust in FRT has been relatively fragile for a number of years. Concerns about accuracy, bias, proportionality, and undisclosed use, particularly in criminal investigations, are well documented. Recent oversight findings and court proceedings have increased expectations around transparency, disclosure, and legal readiness, and court cases increasingly scrutinize whether FRT use was properly documented and disclosed, and whether the technology used was reliable. In some cases, courts have

reversed convictions where FRT use was disclosed too late or was not disclosed in a way that would allow a fair challenge.

4.2 At the same time, guidelines, best practices and standards for responsible FRT deployment, use and management have matured. FISWG has published practical guidance covering the end-to-end lifecycle, from planning and procurement through deployment testing, operational assurance, and post deployment monitoring. In addition, complementary responsible use frameworks reinforce the same general recommendations: defined purpose, necessity and proportionality, human oversight, accountability, and transparency.

5. Significance and Use

5.1 Debate over FRT is no longer about whether scrutiny will occur, but whether agencies are prepared for it. Agencies that embed FISWG aligned assurance practices, adopt clear responsible use governance, and treat transparency as a core design requirement, rather than an afterthought, are better positioned to not only withstand legal challenge, but to demonstrate mature, responsible stewardship of the technology over time. These practices are consistent with the lifecycle-based approach described in the Facial Recognition Technology Implementation Guidelines (v1.0). The recommendations in this document offer a practical path toward that outcome.

5.2 The following sections (Sections 5.2.1–5.2.2.2) describe the operational and governance considerations associated with defensible FRT use, and present structured

recommendations intended to support repeatable, auditable, and transparent implementation.

5.2.1 Litigation and disclosure expectations

5.2.1.1 Recent court decisions demonstrate growing judicial attention to how facial recognition is used, documented, and disclosed. In *Johnson v. State*, 2025 WL , an appellate court reversed a conviction where delayed and incomplete disclosure of facial recognition use prevented the defense from meaningfully challenging reliability. In *State v. Miles*, 2025 WL, building on *State v. Arteaga*, 439 P.3d 1038 (N.M. 2019), amici emphasized the necessity of discovery related to the FRT process and system characteristics when such technology contributes to identification or probable cause.

5.2.1.2 These cases reflect a broader trend: when FRT plays an important role in a case, courts expect agencies to be prepared to explain what was done, using which system, under what conditions, and with what limitations. These judicial expectations mirror concerns raised by oversight bodies and the broader public.

5.2.2 Oversight and public concern

5.2.2.1 Oversight bodies continue to identify gaps in policy and procedures, training, and governance for FRT. Separately, public debate has intensified around proportionality, permanence of deployments, scale of databases searched, and the lack of visibility into how systems are used. Overall, these pressures reinforce the need for agencies to move beyond ad hoc practices and toward a more structured and transparent path.

5.2.2.2 Implication: Agencies should not wait for litigation or oversight findings to define acceptable use of FRT. By adopting established standards and embedding transparency, where possible, into policy, procurement, and operations, agencies can reduce risk and strengthen legitimacy.

5.2.3 Guiding Frameworks

5.2.3.1 FISWG's Responsible Use principles and Operational Assurance series provide stepped, testable practices for responsible FRT deployment, including:

- Purpose definition and use limitations
- Pre and post deployment testing using agency relevant data
- Image quality assessment and threshold setting
- Structured examiner workflows and human review
- Post deployment monitoring and documentation

5.2.3.2 The Facial Recognition Technology Implementation Guidelines (v1.0) extend this approach across a typical FRT system lifecycle, from planning and procurement to ongoing management and review.

5.2.4 Complementary governance frameworks

5.2.4.1 Broader responsible use frameworks adopted by other international organizations reinforce the same core expectations: necessity and proportionality,

human in the loop controls, accountability, data protection, and external transparency. Together, these form a reasonable and practical foundation for agency policy and procedures. These frameworks inform the recommendations that follow, which focus on practical steps agencies can take to operationalize these principles.

6. Recommendations

6.1 The following recommendations are organized by area of focus but are intended to be implemented as a coherent set.

6.2 Legal Readiness and Disclosure

6.2.1 Establish a clear FRT Use and Disclosure Rule

6.2.1.1 Require documentation and timely disclosure, where possible, whenever FRT is used in a way that may contribute to investigative, evidentiary, or operational decision-making, including lead generation, identification, or probable cause. At minimum, records should capture the system used, input image provenance, databases searched, candidate handling, and human review steps. Clear rules help to mitigate risk.

6.2.2 Define a structured discovery protocol

6.2.2.1 Clearly separate information specific to a single case (such as images reviewed, search results, and examiner notes) from information about the system itself

(such as the algorithm version(s), settings, and testing results). This makes explanations easier and avoids confusion during reviews or court proceedings.

6.2.3 Align procurement with legal obligations

6.2.3.1 When procuring FRT, contracts should preserve the agency's ability to meet disclosure, discovery, and audit obligations. Vendors should be required to provide the matching algorithm and version, configuration details, validation and testing results, usage records, and any other information needed to explain system operation and reliability. If some information is sensitive or proprietary, the contract should specify a secure review process so legal proceedings are not delayed or blocked.

6.2.4 Publish an agency level FRT policy and legal basis statement

6.2.4.1 Before deployment, document and make public, where possible, approved use cases, legal authorities, limitations, and prohibited uses. Clear and well-defined policies help protect people's rights and make it easier to explain and defend, in legal proceedings, how the technology was used.

6.2.5 Apply a proportionality and authorization framework

6.2.5.1 Require clear written reasons showing why the technology is needed and whether its use is appropriate for the level of risk involved.

6.3 Operational Assurance and Auditability

6.3.1 Use consistent terminology

6.3.1.1 Agencies should use consistent, well-defined terminology for FRT across operational practice, documentation, and disclosure. Consistent language reduces ambiguity and supports effective audit, oversight, and review. Terminology should, where appropriate, reflect definitions and usage set out in the FISWG Glossary, the Responsible Use principles, the Facial Recognition Technology Implementation Guidelines, and the Operational Assurance document series.

6.3.2 Conduct pre deployment testing using agency data
Validate system performance under actual operating conditions, consistent with FISWG Operational Assurance practices and use results to optimize operational workflows and configuration.

6.3.3 Maintain versioned system records (“algorithm bills of materials”)

6.3.3.1 Keep clear records of which software version was used, how it was set up, what data it used, and how results were produced, so decisions can be verified and reviewed later if needed.

6.3.4 Require training and competency aligned with system use

6.3.4.1 Make sure staff who run searches or review results are properly trained, and receive refresher training.

6.3.5 Preserve comprehensive audit trails

6.3.5.1 Preserve probe images, databases searched, candidate lists, human decisions, and final outcomes. These records support discovery, enable independent review, and provide a basis for ongoing quality assurance and technical oversight.

6.3.6 Monitor performance over time

6.3.6.1 Implement recurring post deployment evaluations to detect performance issues or limitations. Maintain complete documentation of ongoing performance evaluations including any system adjustments.

6.4 Public Transparency and Engagement

6.4.1 Publish a transparency overview

6.4.1.1 Consider sharing easy to understand information about why FRT is used, how it is governed and overseen, and how its accuracy is verified, while leaving out sensitive operational details.

6.4.2 Maintain engagement and accountability mechanisms

6.4.2.1 Establish clear points of contact for questions or complaints and integrate periodic review of FRT use into existing governance structures.

7. Preparations for FRT Case Disclosure Package

7.1 Agencies should plan in advance for the possibility that the use of FRT may be subject to legal, oversight, or public review. Preparing ahead of time helps ensure that the agency can clearly explain without delay how the FRT operates and was applied.

This includes maintaining records and processes that support lawful disclosure, while also allowing sensitive or confidential information to be handled through appropriate safeguards.

7.2 At minimum, agencies should consider having a structured process that includes the following:

7.2.1 Case specific materials

- Probe image(s) and quality metrics
- Databases searched • Candidate lists and similarity scores
- Facial practitioner notes and outcomes

7.2.2 System level information

- Vendor name and algorithm version
- Operating thresholds and score semantics
- Performance summaries and monitoring results

FISWG documents can be found at: www.fiswg.org