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.

Version 1.0 2025.11.21

Facial Recognition Technology Implementation Guidelines

1. Scope

1.1 This document provides guidance for agencies looking to deploy facial recognition technology (FRT). It is not all-encompassing but is broad enough to cover most FRT use cases.

1.2 The document covers the end-to-end process from planning to procurement and ongoing management of the technology.

1.3 This document focuses mostly on technology and not on the role of the human operator. Agencies are encouraged to refer to training and 1:1 FISWG documentation for in-depth guidance on how to train and manage human operators dealing with FRT.

2. Referenced Documents

2.1 *FISWG Standards*:

FISWG Minimum Training Criteria When Using Facial Recognition Systems

FISWG Guide for Facial Comparison Training of Reviewers to Competency

FISWG Principles for Responsible Use of Facial Recognition Technology

FISWG Standard Guide for Capturing Facial Images for Use with Facial Recognition Systems

FISWG Facial Recognition Systems: Operation Assurance Series

3. Terminology

3.1 *Definitions:*

3.1.1 *Algorithm, n*—a set of instructions or steps that tells a computer system how to perform tasks.

3.1.1.1 *Discussion:* In the context of facial recognition technology, facial recognition algorithms detect, analyze, map, and compare faces.

3.1.2 *Facial Recognition System (FRS), n*—a computer system that leverages facial recognition technology.

3.1.2.1 *Discussion:* An FRS contains multiple components (hardware, software, data).

3.1.3 *Facial Recognition Technology (FRT), n*—an algorithm-based technology that compares facial images and produces a resulting similarity score.

3.1.3.1 Discussion: There are two main types of comparisons in an FRT, identification and verification.

3.1.4 *Identification (One-to-Many, 1:N), v*—a task where the facial recognition system searches a facial image against a database and returns a corresponding candidate or candidate list and associated similarity scores.

3.1.5 *Liveness Detection, v*—an algorithm-based technology used to establish and confirm the physical presence of a human being.

3.1.6 *Presentation Attack, n*—the deliberate presentation of a face to a facial recognition system's capture component with the intent of causing it to make an incorrect verification or identification decision.

3.1.7 *Presentation Attack Detection, v*—an algorithm-based technology used to help detect presentation attacks.

3.1.8 *Similarity Score, n*—a value generated by a facial recognition algorithm that demonstrates the amount of similarity between two images.

3.1.9 *Software Development Kit (SDK), n*—a set of tools that allow developers to create software applications.

3.1.9.1 *Discussion:* In facial recognition technology, the SDK houses the algorithm(s).

3.1.10 *Threshold, n*—a numerical value, linked to the similarity score, at which a decision point exists.

3.1.10.1 *Discussion:* In a facial recognition system, a threshold is usually implemented to set a balance between operational efficiency and risk.

3.1.11 *Threshold Score, n—see Threshold*

3.1.12 *Verification (1:1), v*—a task where the facial recognition system compares one facial image to another facial image, resulting in a computer-evaluated similarity score.

3.2 *Acronyms:*

3.2.1 *DET, n*—Detection Error Tradeoff

3.2.2 *FAR, n*—False Acceptance Rate

3.2.3 *FRR, n*—False Reject Rate

3.2.4 *FRS, n*—Facial Recognition System

3.2.5 *FRT, n*—Facial Recognition Technology

3.2.6 *ROC, n*—Receiver Operating Characteristic Curve

3.2.7 *SDK, n*—Software Development Kit

3.2.8 *1:N, v*—One-to-Many

3.2.9 *1:1, v—related to FRS,* One-to-One

4. Significance and Use

4.1 Planning for and deploying a facial recognition system (FRS) is a significant undertaking that can be overwhelming without proper support and guidance.

4.2 This document provides a structured process that agencies looking to deploy a facial recognition system can follow. Following this process will help agencies strengthen the integrity of their deployment, backed by strong foundational documentation.

4.3 This document is relevant for law enforcement, document issuance, and border and immigration control agencies looking to deploy FRT.

4.4 This document is broken into three major phases: Planning, Procurement, and Deployment and Ongoing Management.

5. Procedure

5.1 The planning phase provides a much-needed foundation for the procurement process and supports the agency's use of FRT. A significant amount of planning needs to take place before procurement, and the information in this section can be used to help guide the agency through the planning process.

5.2 **Define Use Case** – The goal of this step is to establish a high-level understanding of how the agency wants to use FRT. This step serves as a foundation for subsequent steps, as the use case dictates the structure and requirements for the planning, procurement and deployment process.

5.2.1 A successful deployment needs to be underpinned by strong foundational documentation specific to the agency’s use case. FRT has many potential use cases. To name a few, it can be used in law enforcement to help generate an investigative lead or help identify persons of interest; in document issuance to help verify the identity of applicants; or in border and immigration control to help verify the identities of travelers.

5.2.2 With so many different potential uses, it is important that agencies understand the specifics of their particular use case and the purpose that the technology will serve. In addition, it is important that the agency understands the problem that they are trying to solve by adopting the technology and ensures that adopting the technology will actually solve this problem.

5.2.3 For this step, agencies are encouraged to draft a workflow specific to the end-to-end FRT process that shows how FRT will be used by the agency and how it will fit into existing agency-specific workflows. An example of a general FRT workflow can be found below in Figures 1 and 2. It should be noted that workflows could include either more or less than what is depicted in the figures 1 and 2.

5.2.4 Outcome – At the end of this step, agencies should have defined their respective FRT use case and developed high level documentation that outlines the purpose the technology will serve and how it will fit into existing agency processes and frameworks.

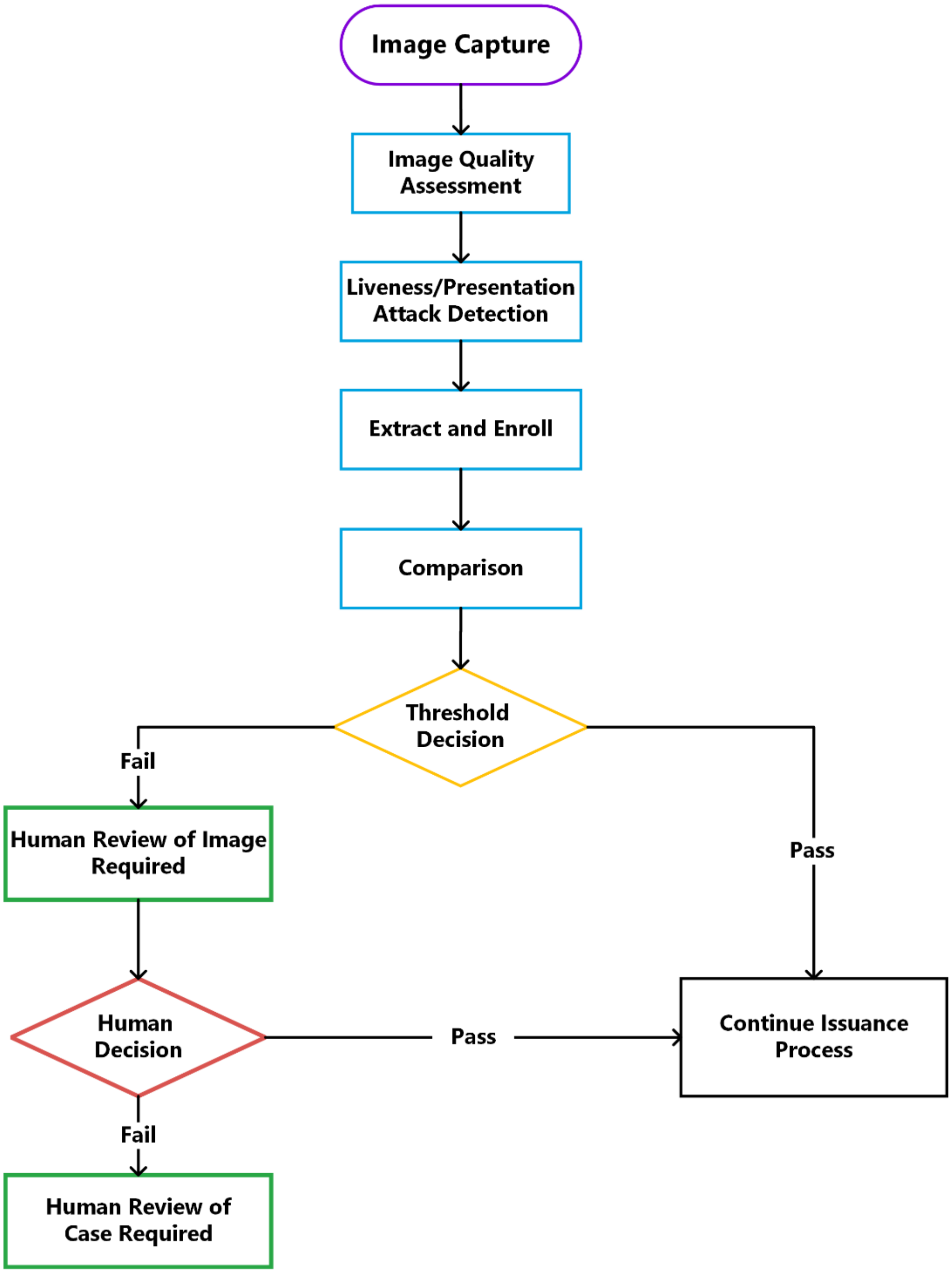
Image Capture
Image Quality Assessment
Liveness/Presentation Attack Detection
Extract and Enroll
Comparison
Threshold Decision
Fail
Pass
Human Review of Image Required
Human Decision
Pass
Continue Issuance Process
Fail
Human Review of Case Required

Figure 1: High Level FRT Flow – Document Issuance

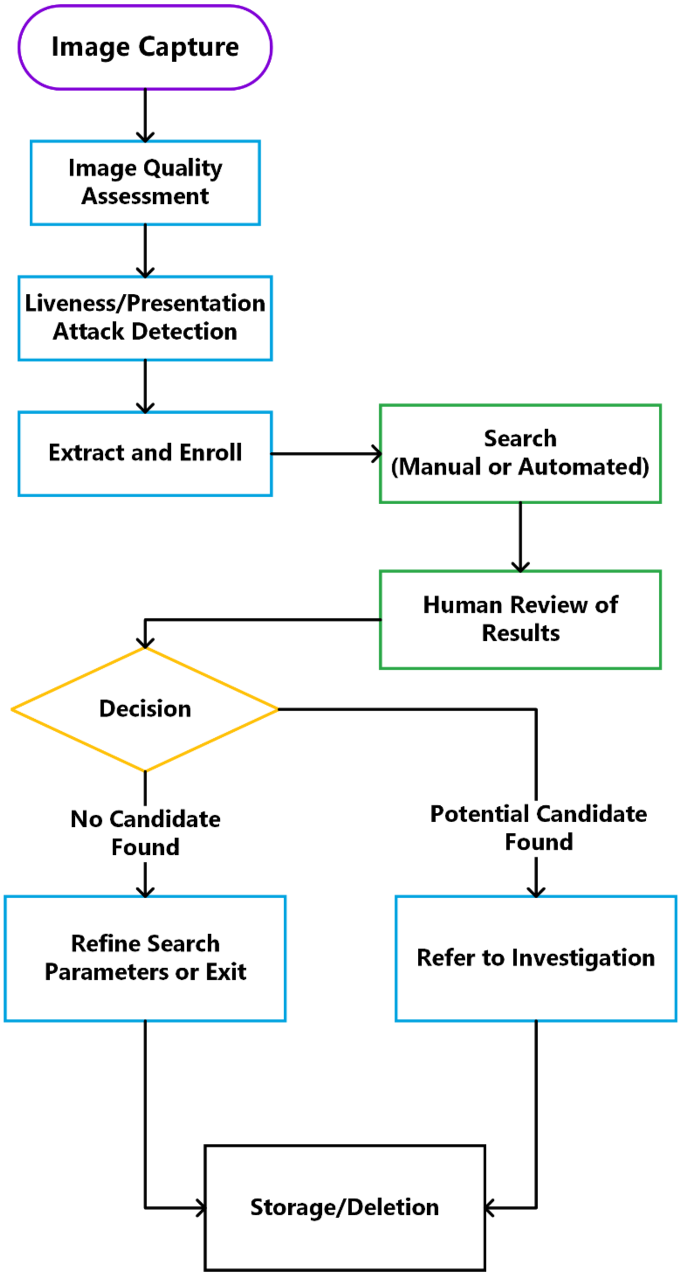

Figure 2: High Level FRT Flow – Law Enforcement, Border and Immigration

5.3 **Ethical Considerations** – The goal of this step is to discuss and document ethical considerations related to the agency's use of FRT. Considering ethics early on in the deployment process will help the agency understand what type of ethical considerations apply to their specific use case. And this information can be used to help shape policy and procedures and ensure that public engagement is captured and transparent. Additionally, the content in this section is based on many other guidelines and frameworks[1], which agencies can also leverage.

5.3.1 There are several ethics-related components to consider when looking to deploy FRT. The considerations in this area will differ depending on the use case and region. For example, an agency may need to comply with overarching guidance documents when looking to deploy FRT – and these documents often contain ethical considerations specific to FRT (e.g., EU AI Act, Illinois Biometric Information Privacy Act).

5.3.2 Agencies are encouraged to research how each of the following areas may apply to their specific use case, in their specific region, to determine if they need to include requirements related to ethics in their deployment project:

5.3.2.1 Human Rights – Does your proposed use of FRT align with relevant human rights legislation and regulations?

5.3.2.2 Consent – Do you need consent to collect and enroll your client data into an FRS?

5.3.2.3 Surveillance – Does your use case involve surveillance? If it does, does policy, legislation, and regulations in your region support this type of use?

5.3.2.4 Privacy – Do relevant legislation, regulations, and policies related to privacy support your proposed use of FRT?

5.3.2.5 Security – What type of steps do you need to take to protect the biometric information of your clients and to protect your clients' data from attacks?

5.3.2.6 Bias – How might potential bias impact your clients? How can you limit the presence of bias in your end-to-end FRT process?[2]

5.3.3 Outcome – At the end of this step, agencies should have documentation showing how they have taken ethics into consideration during the design and deployment of FRT. This documentation will help shape policies and procedures and will help ensure that agencies have taken the necessary steps towards using FRT responsibly with the necessary guardrails in place.

5.4 **Governance** – The goal of this step is to ensure that the agency has the authority to use FRT and that the use is well supported by relevant legislation, regulations, policies, and procedures. When the use of FRT is supported by strong

[1] https://www.weforum.org/publications/a-policy-framework-for-responsible-limits-on-facial-recognition-use-case-law-enforcement-investigations-revised-2022/; https://www.biometricsinstitute.org/the-three-laws-of-biometrics/

[2] More information on this consideration can be found in the testing section of this document.

documentation, risk is minimized, public acceptance is greater, and the path to deployment is smoother.

5.4.1 Legal Authority, Legislation, and Regulations – Ensuring that the agency has the legal authority, and its use is supported by relevant legislation and regulations is a fundamental beginning step in the facial recognition acquisition and deployment journey. Early engagement with your Legal services team to discuss the use case is critical to ensure the FRT is used in a legally compliant and ethical manner to achieve agency aims on necessity and proportional use. Documentation of progress and discussions in this area establishes if the technology can be used and if so, how it can be used in compliance with the law. Understanding the implications of relevant legislation and regulations at the beginning of a deployment project can help agencies ensure that they build the FRS in a way that aligns with this documentation – reducing the probability of complications in this area and increasing the likelihood of a successful and compliant deployment.

5.4.2 Policy – Once the agency has determined that their use of FRT will comply with relevant legislation and regulations, the next step is to review and/or develop policies that will define how the technology can be used by the agency. Defining how technology can be used is an essential step that should be taken before procurement and subsequent deployment. Understanding how the technology will be used will help the agency develop business requirements that meet their needs, guided by strong policy. Existing policies should be leveraged, where possible. If policies do not exist that cover the use of FRT, the agency should consider drafting new policies or adopting and modifying policies from other agencies that share similar mandates. As policy can take a long time to draft, it is recommended that the agency start work in this area as soon as possible.

5.4.2.1 It is important to note that the agency should consider policy from several different areas when working through an FRS deployment. Many different stakeholders are involved with a typical deployment process, so agencies should ensure that policies from all areas are considered (procurement, risk management, finance, organizational alignment, privacy and ethics, information management, security, identity management, biometrics, emergency management, information sharing, standards, training, and support). The aforementioned list can also be leveraged to assign the necessary stakeholders to the deployment project.

5.4.3 Procedures – Drafting detailed procedures on exactly how the technology will be used helps ensure compliance with legislation, regulations, and policy. In addition, detailed procedures help ensure that all technology operators will use the technology in a consistent way. Role-based access controls are useful to ensure access is managed at a user and administrator level. Consistent use of the technology across the agency increases the likelihood that the technology will be used responsibly and in line with standards and best practices, which limits risk.

5.4.3.1 The agency should consider drafting procedures for each stage of the end-to-end FRT process. Agencies are encouraged to use Figure 1 and 2 in Section 5.1 as a reference to help develop procedures for each step in the process flow.

5.4.4 Outcome – At the end of this step, agencies should have gathered (or drafted) legislation and regulations that give them the authority to use FRT; gathered or drafted policies that define how the technology can and will be used; and drafted procedures – to the extent possible – that detail how each type of user will use the FRS. This documentation will help agencies plan subsequent phases of the deployment and can be leveraged to show that the technology is being used responsibly, consistently, and in line with relevant legislation, regulations, policies, and procedures.

5.5 **Communications Strategy** – The goal of this step is to draft a Communications Strategy that will create the narrative for the deployment project and serve as a method to communicate information about the deployment to relevant stakeholders and the media.

5.5.1 Stakeholder Communication – From a stakeholder perspective, clear and concise communication keeps stakeholders in the know and helps increase buy-in from employees, management, and other stakeholders. As a whole, this will help ensure that the deployment project runs as smoothly as possible and that risks related to misunderstanding will be limited. In addition to clear and concise communication, agencies could also consider a feedback mechanism for stakeholders. Gathering feedback during a deployment project can help identify issues, improve project relationships and further mitigates the risk of issues.

5.5.2 Media Communication – Agencies should expect questions from the media or general public and, where possible, should prepare a strong external communications package that can be leveraged to help respond to these questions. The communications package should be clear and concise and should be based on terminology from a recognized source[3]. Consistent terminology helps limit misunderstandings and ensures that the right message makes it to the right people at the right time.

5.5.3 Communications Package Strategy – In terms of strategy, the agency could consider drafting a Frequently Asked Questions (FAQ) document that could be leveraged for both stakeholder and media communications purposes. The FAQ document could contain questions and answers about the technology in general and more specific questions and answers related to the deployment project and the agency's use case. It could also contain "myth busting" statements that help correct misconceptions around the technology. FISWG's FAQ document can serve as an example: https://fiswg.org/faq.html.

[3] Consistent terminology sources: FISWG Glossary and ISO Harmonized Biometrics Vocabulary: ISO/IEC 2382-37:2022

5.5.4 The outcome of this step is for the agency to possess documentation that can be leveraged to promote clear and consistent messaging about FRT in general and the agency's deployment project to relevant stakeholders. Clear and transparent communication (where possible) will help build trust in the technology, which will help the biometrics community as a whole.

6. Procurement

6.1 The goal of this phase is to provide a high-level overview of the procurement process via a breakdown of each of the below-mentioned components, which will help the agency plan for an effective and efficient deployment.

6.1.1 Any acquisition of FRT will likely have to go through a formal procurement process. Procurement process structure can vary per region, but, in general, the following components may be included:

6.1.1.1 Project Plan

6.1.1.2 Risk Management Plan

6.1.1.3 Business Case

6.1.1.4 Requirements Gathering

6.1.1.5 Request for Information (RFI)

6.1.1.6 Request for Proposal (RFP)

6.1.1.7 Vendor and Technical Evaluation

6.1.1.8 Negotiate Contract

6.1.1.9 Build and Test

6.1.1.10 Deploy

6.1.1.11 Review

6.2 Procurement Components and Associate Steps

6.2.1 **Create Project plan** – The first step in the procurement process phase is to create the project plan. The plan communicates a clear vision for project objectives and tasks, maps project resources and roles, organizes project-related work and defines goals, timelines and high-level budget. This document gives much needed structure to the project. See Table 1 for additional guidance on creating a project plan.

Task:	Guidance:
Define Project Scope and Goals	• Clearly outline what the project aims to achieve, what it will not achieve, and its boundaries. • Ensure goals are SMART (Specific, Measurable, Achievable, Relevant, Time-bound)[4].
Identify Stakeholders and Roles	• List all stakeholders and define their roles and responsibilities and to whom they report.
Set Budget	• Estimate costs for resources, work, and contingencies. • Monitor and adjust the budget on an as needed basis.
Create Timeline and Schedule	• Break the project into tranches and set milestones. • Use tools to help visualize the timeline (Gantt Chart).
Outline Deliverables and Key Milestones	• Define what needs to be delivered and when. • Ensure that deliverables are aligned with the project goals.
Plan for Resources	• Identify the resources (financial, human, material) required. • Ensure that resource availability aligns with the project timeline.
Communication Plan	• Establish how and when updates will be communicated to stakeholders. • Ensure clear and consistent communication channels.[5]
Quality Management	• Define quality standards and how they will be measured. • Implement regular quality assessments and reviews
Review and Adjust	• Regularly review project progress and make necessary adjustments. • Be flexible and responsive to changes.

Table 1: Create Project Plan Tasks

[4] https://www.techtarget.com/whatis/definition/SMART-SMART-goals

[5] Communications Strategy from 5.4 should be leveraged here.

6.2.2 **Create Risk Management Plan** – The second step in the procurement process is to create a risk management plan. The risk management plan should include all potential risks related to each step of the procurement process. It should be all-encompassing, and it should be reviewed and updated on a regular basis. See table 2 for additional guidance on creating a risk management plan.

Task:	Guidance:
Identify Risks	• Define potential risks that could impact the procurement.
Analyze Risks	• Evaluate the probability and impact of each risk.
Prioritize Risks	• Rank risks based on their probability and impact.
Mitigation Strategies	• Develop plans on how to reduce or eliminate risks, where possible.
Assign Tasks and Responsibilities	• Designate stakeholders to manage each risk.
Monitor and Review	• Regularly review and update the risk management plan.
Communication Plan	• Ensure all stakeholders are regularly informed and updated about risks and their status.
Contingency Plans	• Prepare plans for how to respond to risks should they occur.
Documentation	• Keep detailed records of all risk management activities and keep these records up to date.[6]

Table 2: Create Risk Management Plan Tasks

6.2.3 **Develop Business Case** – The third step in the procurement process is drafting the business case, which highlights how the agency will use FRT and details their needs. The business case forms the justification for the FRS and serves as the basis for the following steps within the procurement phase. See Table 3 for additional guidance on drafting a business case.

Task:	Guidance:
Identify the Business Problem	• Clearly define the issue that the project aims to address.
Outline Options	• Present different options that can potentially solve the problem, including their pros and cons.

[6] Risk Management Plan template examples: Risk Management Framework (RMF): Definition and Components (www.investopedia.com) and https://csrc.nist.gov/pubs/sp/800/37/r2/final

Recommend the Best Option	• Justify why the chosen option is the most effective.
Executive Summary	• Provide a brief overview of the business case that highlights key points.
Cost-Benefit Analysis	• Detail the financial implications, including costs, benefits, and expected return on investment.
Risk Assessment	• Identify potential risks and risk management strategies.
Implementation Plan	• Outline the steps, timeline, and resources required to execute the project.[7]
Stakeholder Analysis	• Identify key stakeholders as well as their role in regard to the technology.[8]
Performance Metrics	• Define how success will be measured and monitored.
Conclusion	• Summarize the key considerations and reiterate the recommendation.

Table 3: Business Case Tasks

6.2.4 **Requirements Gathering** – The fourth step in the procurement process is to turn the aforementioned business case into a set of requirements that can be clearly communicated to relevant stakeholders and used in the vendor solicitation process. See Table 4 for additional guidance on requirements gathering.

Task:	Guidance:
Clear Objectives	• Ensure that the purpose of the project is clear and that the use case is well defined and understood.
Stakeholder Involvement	• Engage with stakeholders to gather their requirements and expectations.
Specific and Measurable	• Ensure requirements are detailed, specific, and measurable.
Prioritization	• Rank requirements based on their level of importance.
Scope Definition	• Outline what is included and excluded from the project. Be clear and concise.
Feasibility	• Determine the technical and financial feasibility of the requirements.
Consistency	• Maintain consistency in terminology, format and style throughout the document.

[7] Agency can leverage Project Plan (6.2.1) for this step.

[8] Agency can leverage Project Plan (6.2.1) for this step.

Traceability	• Ensure that each requirement can be traced back to business objectives.[9]
Validation and Verification	• Include methods for validating and verifying the requirements.[10]
Change Management	• Establish a plan for how changes to requirements will be managed.

Table 4: Requirements Gathering Tasks

6.2.5 **Request for Information (RFI)** – The fifth step in the procurement process is to conduct market research to determine potential technologies and vendors that may meet agency requirements. This is done through a formal document and process referred to as "Request for Information (RFI)." The RFI mechanism allows the agency to "see what's out there" and provides an opportunity to hear from vendors who think they may be able to meet agency needs. See Table 5 for additional guidance on RFIs.

Task:	Guidance:
Objective	• Define the purpose (e.g., law enforcement, access control).
Scope	• Specify deployment areas and environments and explain the use case.
Users	• Identify primary users.
Technical Specs	• Detail requirements pertaining to capture station, processing power, architecture (bare metal or cloud), software development kit (SDK), algorithm(s) – FRT, image quality, presentation attack detection – and integration needs.
Accuracy	• State required accuracy and performance metrics and ask vendors to provide evidence of claims on system accuracy and equitability.
Privacy	• Outline requirements for data protection and compliance with privacy laws.
User Interface	• Describe expected user experience.
Integration	• Specify integration with existing systems.
Security	• Define security requirements for technology, architecture, and employees.
Support	• Detail maintenance and support requirements.

[9] This can be achieved through a Traceability Matrix: https://www.wrike.com/blog/what-is-requirements-traceability-matrix/

[10] Distinction between terms can be found here: https://www.geeksforgeeks.org/differences-between-verification-and-validation/

Cost	• Provide budget range and request cost breakdowns.
Vendor Experience	• Request case studies or references.
Compliance	• Ensure compliance with industry standards.
Testing	• Outline requirements around testing and evaluation process.
Timeline	• Provide project timeline and milestones.
Demo	• Consider vendor demos to give vendors the opportunity to show their products and explain how they can meet agency needs.
Contact	• Include contact details for follow-up.

Table 5: RFI Tasks

6.2.6 **Request for Proposal (RFP)** – The sixth step in the procurement process is to put together a package that outlines the agency requirements and information gained from the Request for Information to solicit bids from interested vendors. See Table 6 for additional guidance on RFPs.

Task:	Guidance:
Objective	• Define the purpose for the procurement (e.g., to assist with identity management at the border).
Scope	• Specify deployment areas and environments.
Users	• Identify primary users.
Technical Specs	• Detail camera resolution, volume, processing power, and integration needs.
Accuracy	• State required accuracy and performance metrics. • Make it mandatory that vendors provide evidence of claims on system accuracy and equitability.
Privacy	• Outline privacy and data protection needs.
User Interface	• Describe expected user experience.
Integration	• Detail any required integration with existing systems.
Support	• Define maintenance and support requirements.
Cost	• Provide budget range and request cost breakdowns.
Vendor Experience	• Request case studies or references.
Compliance	• Ensure compliance with industry standards (ISO, ANSI/NIST, etc.).

Timeline	Provide project timeline and milestones.
Contact	Include contact details for follow-up.

Table 6: RFP Tasks

6.2.7 **Vendor Evaluation** – The seventh step in the procurement process is to evaluate bids that were received from vendors during the RFP process. See Table 7 for additional guidance on vendor evaluation.

Task:	Guidance:
Performance	National Institute of Standards and Technology (NIST) Face Recognition Technology Evaluation (FRTE)[11] results should be reviewed, at the very least. A combination of reviewing NIST results and testing on operational ground truth data would be preferred. If possible, evaluate false positive and false negative rates of the respective algorithm – in general and across different demographics (sex, skin tone, race, age).
Compliance	Ensure the technology complies with relevant legislation and regulations, including those pertaining to ethics and privacy.
Security	Assess the effectiveness of data encryption and storage solutions. Review vendor methods for data breaches.
Scalability and Integration	Determine if the technology can scale with agency needs. Determine compatibility with existing agency systems and architecture.
User Experience and Support	Evaluate the ease of use for end-users. Consider the quality and availability of vendor support and training.
Cost and Licensing	Determine the cost of ownership, including setup, support, maintenance, and possible enhancements. Review licensing terms for flexibility and fairness.

[11] https://www.nist.gov/programs-projects/face-technology-evaluations-frtefate

Vendor Capability	• Research the vendor’s reputation in the market.[12] • Consider conducting site visits to observe the use of the algorithm or system and acquiring references.
Transparency and Accountability	• Ensure the vendor provides clear and concise documentation that shows transparency of their processes and methods. • Ensure that there is a mechanism for independent audits and assessments

Table 7: Vendor Evaluation Tasks

6.2.8 **Negotiate and Aware Contract** – The eighth step in the procurement process is to select the winning bidder based on the vendor evaluation and to define contract terms. See Table 8 for additional guidance on negotiation and awarding the contract.

Task:	Guidance:
Scope of work	• Clearly define deliverables, timelines, responsibilities, and overall expectations. • Ensure project milestones and any performance metrics are detailed.
Pricing and Payment Terms	• Negotiate total cost and payment schedule. • Define any additional costs, such as support and maintenance fees.
Confidentiality and Security	• Include clauses to protect intellectual property and protected or confidential information. • Ensure compliance with security and data protection regulations.
Warranties and Liabilities	• Define warranty coverage and conditions. • Establish liability clauses – relating to losses or damage incurred by either party.
Contract Termination	• Outline contract termination conditions specific to each party. • Define adequate notice periods and any associated penalties or fees.
Dispute Resolution	• Agree on a dispute resolution mechanism, such as mediation. • Include references to governing law for legal matters.

[12] This can be done via online searches for case studies or testimonials but can also be done through discussions with partners that use the same vendor.

Performance Standards and Penalties	- Set clear expectations for performance standards and metrics. - If possible, consider defining penalties for failure to meet agreed-upon standards.
Change Management	- Establish procedures for handling changes to contract terms or work scope. - Include provisions for contract amendments, timeline extensions, and cost adjustments.
Support and Maintenance	- Detail the level of support and maintenance services provided. - Specify expected issue response and resolution times. - Include specifications around algorithm upgrades throughout the lifetime of the contract.
Review and Approval Process	- Ensure thorough review and approval by all relevant stakeholders.

Table 8: Negotiate and Award Contract Tasks

6.2.9 **Build and Test** – The ninth step in the procurement process is to work with the new vendor to build, test, and integrate the FRS into existing agency architecture and processes, where needed. The information from the business case and contract terms sections should be referenced. See Table 9 for additional guidance on building.

Task:	Guidance:
Stakeholder Engagement	- Involve stakeholders from all relevant areas (IT, User Groups, Security, Legal, etc.).[13] - Ensure that a feedback loop exists for stakeholders to voice their opinions and concerns during the build process.
Requirements	- Refine requirements around accuracy, including acceptable false positive and false negative rates and ability to adjust threshold. - Further define use case, such as security, access control, or customer identification.[14] - Ensure that the system is built with specific agency use case in mind.
System Architecture	- Design for scalability to handle varying volumes of data and users.

[13] Resource portion of Project Plan (6.2.1) can be leveraged here.

[14] Agency can leverage work done in Planning Phase (5.1) here.

	• Ensure compatibility with existing security and IT infrastructure. • Consider building a pre-deployment testing environment to allow end-to-end testing before deployment.
Security and Compliance	• Implement strong encryption for data transmission and storage. • Ensure compliance with relevant legislation, regulations, and laws.
Data Quality and Bias Mitigation	• Use (or ensure that the vendor used) diverse and operationally relevant datasets to train the system and reduce bias. • Where possible, regularly audit the system for performance across different demographic groups.
Data Migration	• Plan for secure migration of existing data. • Validate data integrity and accuracy post-mitigation.
Testing and Quality Assurance	• Conduct extensive testing, including real-world scenarios (both common and uncommon). • Perform user acceptance testing to ensure the system meets user needs. • Validate end-to-end system performance prior to deployment (from data capture to deletion).
Training and Documentation	• Provide training for end-users and administrators on FRS use and best practices. • Develop comprehensive documentation for system operation and troubleshooting. This is often in the form of user guides.
Change Management	• Prepare a change management plan to support user adoption and reduce the likelihood of resistance. • Communicate changes effectively to all stakeholders.
Performance Metrics	• Define key performance indicators (KPIs) such as image quality, recognition accuracy, processing speed, and user satisfaction.

Table 9: Build and Test Tasks

6.2.10 **Deploy** – The tenth step in the procurement process is to deploy the new FRS into production. See Table 10 for additional guidance on deployment.

Task:	Guidance:
System Configuration	• Ensure proper setup and calibration of hardware and software. • Verify successful integration with existing systems and infrastructure.
Data Security	• Ensure robust encryption for data storage and transmission is active and working as intended. • Ensure ongoing compliance with relevant data protection legislation and regulations.
User Training	• Complete any remaining or outstanding training for end users or system administrators. • Leverage easy-to-follow guides and documentation mentioned in Build step (6.2.9).
Privacy and Ethical Considerations	• Monitor that user consent and transparency in data usage policy and procedures are being followed. • Monitor that ethical considerations raised during the project planning and procurement phases of the project are being followed. • Address issues found during monitoring.
Monitoring and Support	• Ensure that appropriate resources (as defined earlier in the document) are assigned to system-related tasks. • Set up continuous monitoring for system performance and security. • Leverage support and maintenance agreement and related procedures to handle any bugs or issues post-deployment.
Feedback Mechanism	• Implement a system for collecting user feedback. • Use feedback to make necessary adjustments, improvements, and enhancements. • Feedback can also be obtained through audits or reports obtained from the pre-deployment environment.

Table 10: Deploy Tasks

6.2.11 **Review** – The last step in the procurement process is to conduct an analysis of the success of the procurement process and subsequent deployment and use the analysis to draft lessons learned. See Table 11 for additional guidance on reviewing.

Task:	Guidance:
Contract Compliance	• Ensure all contract terms and conditions have been met by both parties.
Performance Evaluation	• Assess the performance of the vendor against key performance indicators (KPIs) and agreed-upon deliverables.
Cost Analysis	• Review costs incurred and compare them against the initial budget and forecast.
Quality Assurance	• Verify that the goods or services received meet the required quality standards.
Documentation	• Ensure all procurement documents are complete, accurate, and properly archived for future reference.
Stakeholder Feedback	• Gather feedback from all stakeholders involved to identify any issues or areas for improvement.
Lessons Learned	• Document lessons learned throughout the procurement process to leverage for and enhance future projects.
Final Payments	• Confirm that all necessary payments have been made as per contract terms.
Regulatory Compliance	• Ensure all procurement activities comply with relevant laws and regulations.
Project Closeout Report	• Prepare a detailed closeout report that summarizes the procurement process, outcomes, and any recommendations for future projects.

Table 11: Review Tasks

6.3 Outcome – At the end of this step, by following the guidance above, the agency should have completed the procurement process, backed by strong foundational documentation, and in line with biometrics standards and best practices.

7. Ongoing Management

7.1 The goal of this phase is to ensure that the agency is well prepared to manage the new FRS on an ongoing basis. Ongoing management of the new FRS involves several tasks – namely: support and maintenance, performance measurement, and enhancements. This section of the document will provide an overview of these tasks, which will help the agency prepare for post-deployment activities.

7.1.1 **Support and Maintenance** – Ongoing support and maintenance is essential to ensuring that the FRS is functioning as intended and as was defined in the contract. Following deployment, the agency and the vendor must work together following the terms and conditions set out in the Support and Maintenance Plan that was established during the contract stage of the procurement process.

7.1.1.1 Ideally, the contract would permit 24/7 support, which would ensure that any bugs or issues are addressed immediately, regardless of time or day. In addition, the Support and Maintenance Plan should detail a clear and concise escalation process and a timeframe for fixes.

7.1.1.2 Procedural documents mentioned above should detail the process that different users need to take to identify a bug or issue, and a clear communication channel should also be established. In addition, architectural documents (both internal and vendor-related) should define and support bug and issue fix procedures.

7.1.2 **Performance Measurement** – Ongoing system and algorithm performance measurement helps the agency prove that the FRS is working as per the requirements set out in the FRS vendor contract. It also helps the agency prove that they are in compliance with facial recognition standards and best practice documents that stress the performance of "knowing your algorithm." Where possible, the agency should strive to conduct ongoing performance measurement – either through the FRS vendor, or in-house. In addition, performance testing should be conducted using operationally relevant data and sample sizes. See Table 12 for additional guidance on performance measurement.

Task:	Guidance:
Regular Audits and Reporting	• Scheduling regular audits and reporting of system and user performance can help inform research needs. • Audits and reporting should become an ongoing task for the FRS business owner.
Accuracy and Reliability	• Ensure the system consistently identifies individuals correctly and minimizes false positives and negatives. • Consider comparing results to baseline testing from initial performance measurement to ensure consistency or improvements.
Bias and Fairness	• Regularly check for and mitigate any biases that may exist based on clientele (age, race, sex).

Security	• Monitor for vulnerabilities that could be exploited and ensure data protection measures are up to date.
Compliance	• Stay aligned with evolving legal and regulatory requirements related to privacy and data protection.
Adaptability	• Update the algorithm to handle new data and changing conditions effectively. • Any algorithm upgrades should go through rigorous testing to ensure the new algorithm version meets agency requirements around accuracy, fairness, and speed.
User Feedback	• Collect and analyze feedback from users to identify areas for improvement.
Performance Metrics	• Track key performance indicators (KPIs) such image quality, processing speed, accuracy rates, and error rates.
Scalability	• Ensure the system can handle increased loads and larger datasets as usage grows.
Environmental Changes	• Adapt to changes in the environment where the system is deployed, such as lighting or camera angles.
Ethical Considerations	• Continuously evaluate the ethical implications of the system's use and its impact on society.

Table 12: Performance Measurement Tasks

7.1.2.1 These considerations help maintain the system's effectiveness, fairness, and security over time.

7.1.3 **Enhancements** – Technology advances at a rapid pace, so the agency should plan for enhancements – outside of bug and issue fixes – on a regular, and perhaps even cyclical basis. Without the ability to enhance, the FRS will become outdated. See Table 13 for a list of potential enhancements to consider.

Task:	Guidance:
Software Updates	• Regular updates to improve accuracy, security, and performance.
Hardware Upgrades	• Enhancing capture equipment to improve image quality, enhancing processing equipment and workstations to improve research and user satisfaction/productivity.

Algorithm Upgrades	• Frequent algorithm version upgrades to increase accuracy and reduce bias.[15]
Data Security	• Strengthening data encryption and access controls.
User Interface Enhancements	• Improving user experience and ease of use.
Compliance Updates	• Ensuring the system meets new regulations and standards.
Training and Support	• Providing ongoing training for users and support staff.
Scalability	• Ensuring the system can handle more data, users, and new technology.
Integration	• Enhancing integration with other systems[16] and platforms.

Table 13: Potential Enhancements

7.2 At the end of this step, the agency should be well-prepared to manage the new FRS in line with important standards and best practices and be confident that their use of FRT was implemented in a responsible manner.

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

[15] The agency should use NIST FRTE results as a benchmark and test on operationally relevant data before upgrading.

[16] Such as identity management systems, case management systems, or issuance systems.

ANNEX

(Mandatory Information)

A1. Biometric Performance Measurement Methods

A1.1

Biometric Performance Measurement Methods	
1:1 - Verification The comparison of a facial image to another image, resulting in a computer-evaluated similarity score. This helps answer the question: "Is this the same person?" *	Measures the performance of a FRT algorithm on the Verification task – one probe compared to a reference or other probe. Testing methods used: Determining False Match Rate (FMR) at a specific False Non-Match Rate (FNMR). Confusion Matrix, Receiver Operating Characteristic Curve (ROC), Detection Error Trade-off Curve
1:N – Identification A task where the facial recognition system searches a facial image against a database and returns a corresponding candidate or candidate list and similarity scores. This helps answer the question: "Who is this person?" *	Measures the performance of a FRT algorithm on the Identification task – one probe compared to a database of reference templates. Testing methods used: Determining False Negative Identification Rate at a specific False Positive Identification Rate (FPIR). Rank-Based Analysis - Cumulative Match Based Characteristic Curve (CMC).
Presentation Attack Detection	Refer to ISO/IEC – 30107-1 for performance testing methodology in this area.

*See FISWG Facial Recognition System: Operational Assurance Series