Equality Impact Assessment [EIA]

Section 1: LFR deployments

Background

Live Facial Recognition (LFR) technology is becoming more widely used by law enforcement as a tool to assist officers to locate individuals of interest. Immigration Enforcement (IE) is seeking to use LFR as a precision, intelligence-led tactic to help locate individuals who meet authorised, objective and pre-defined watchlist criteria for the specific deployment, where there is a clear lawful basis, operational necessity and documented proportionality assessment.

Only individuals who fall within **strict, objective and predefined categories** may be included on an LFR watchlist. The eligible groups set out in the IE LFR Policy are:

- Persons subject to an extant Deportation Order made under immigration legislation.
- Persons wanted on a warrant issued by a court in the United Kingdom in relation to an immigration-related offence.
- Persons sought in relation to a charge or charges following a formal decision to seek their attendance or arrest in connection with a criminal immigration-related offence.
- Persons liable to detention under immigration legislation.
- Persons currently and actively sought for enforcement and/or removal action by Immigration Officers.
- Persons who have failed to comply with immigration conditions of entry or stay or lawful removal directions.

LFR technology uses biometric data to compare faces in the camera's field of view with an authorised watchlist. Any alert must be reviewed by trained officers before any engagement or further action is considered.

LFR is a decision-support tool used to assist trained officers in deciding whether to engage and examine a potential person of interest during an otherwise authorised business-as-usual CROP (Crime Reduction Operation), STOP (Street Operation), Holyhead-type or comparable operation. An LFR alert does not confirm identity, establish an immigration breach or offence, or confer any independent power to stop, question, arrest or detain. This EIA assesses only the additional equality impacts arising from the use of LFR. Any subsequent engagement, examination or operational action is governed by the applicable statutory powers, AD booklet, published IE guidance, operational EIA, authorising documentation and safeguarding arrangements for the underlying operation. This EIA must be read together with those documents.

Despite its benefits, facial recognition technology raises concerns regarding privacy, accuracy, bias and potential misuse. Privacy advocates have

highlighted the risks associated with mass surveillance and the collection of sensitive biometric data without informed consent, and these issues have contributed to public concern. For LFR deployments, Immigration Enforcement will use watchlist images that have been lawfully collected and retained.

The legal challenges for facial recognition mostly stem from Article 8 of the European Convention on Human Rights (ECHR). That Article provides:

Right to respect for private and family life

1. *Everyone has the right to respect for his private and family life, his home, and his correspondence.*
2. *There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*[1]

IE recognises the importance of addressing public concern regarding the right to private life. We aim to achieve this by using LFR technology only where it is justified, transparent and impactful. Assessed information may inform where and when LFR is deployed, but inclusion on a watchlist must be based on authorised, objective and pre-defined watchlist criteria for the specific deployment. Clear signage will be used during deployments to support public awareness and understanding.

IE will only process the minimum amount of data necessary to support LFR deployments targeted at individuals who meet the authorised watchlist criteria for the specific deployment, where there is a current, lawful immigration enforcement or criminal law enforcement purpose and a documented necessity and proportionality assessment.

Biometric data that does not generate an alert is automatically and permanently deleted as part of the live process. Where an alert is generated, IE will retain only the minimum LFR information necessary for immediate verification, audit and assurance, and will delete operational LFR artefacts within the period specified in the Written Authority Document and Deployment Record, normally within 24 hours. No biometric template will be retained beyond live processing. Anonymised or de-identified information may be retained where lawful, necessary and proportionate to monitor accuracy and equality impacts. Any separate case or CCTV record arising from a subsequent encounter is governed by the retention requirements applicable to the underlying operation.

[1] Human Rights Act 1998

Watchlists will be subject to pre-deployment quality assurance to confirm that they meet the authorised watchlist criteria, that they remain current, lawful, necessary and proportionate, and that the images used are suitable and lawfully held.

We will undertake a post-deployment debrief, review the results, and publish the number of faces processed by the LFR system, confirmed matches and false alerts.

LFR Deployment

LFR will assist officers to locate individuals who meet the authorised watchlist criteria set out in the IE LFR Policy.

LFR does not confirm identity or determine whether an offence has been committed or whether a person may be subject to administrative enforcement action. It generates a potential alert for trained officer review, after which any engagement or further action must be supported by a lawful basis and further identity checks.

Deployment locations will be selected on the basis of intelligence, threat, harm, operational necessity and proportionality. Locations will not be selected because of the race, nationality, ethnicity, religion or any other protected characteristic of people likely to be present. Each deployment will require a documented rationale and authorisation explaining why LFR is necessary and proportionate in that location, at that time, and for the relevant authorised watchlist criteria.

LFR Technical Process

LFR works by measuring and comparing key facial features. It turns a face image captured by the deployment cameras into a set of numbers, known as a biometric template, and compares that template with templates in an authorised watchlist to find possible matches.

If the system finds a possible match, it generates an alert. A trained operator reviews the alert and decides whether it may be a match. Engagement officers carry out further checks and decide whether any action is then required. LFR supports staff decision-making; it does not make decisions by itself.

Although the technology is assessed as highly accurate when operated at the authorised threshold, zero misidentifications cannot be guaranteed. Misidentification risk will be managed through threshold setting, trained operator review, engagement officer checks and post-deployment monitoring.

IE will undertake its own LFR deployments using IE-owned equipment operated by appropriately trained IE staff. The technology selected for IE-led deployments is also used by authorised LFR-equipped police forces and has been subject to independent operational testing by the National Physical Laboratory. IE may additionally undertake joint deployments with authorised law-enforcement partners where operationally appropriate.

The NPL is a world-leading centre of excellence that provides cutting-edge measurement in science, engineering and technology. Previous testing by the National Institute of Standards and Technology (NIST) showed MPS and SWP that their FRT used a high-performing algorithm. The operational testing aimed to develop an in-depth understanding of the algorithms' performance in operational environments.

The three policing use cases analysed were:

- Live Facial Recognition (LFR)
- Retrospective Facial Recognition (RFR)
- Operator Initiated Facial Recognition (OIFR)

The NPL testing was specifically designed to help identify any impact this technology may have on any protected characteristics, in particular race, age and sex.

The NPL report gives an impartial, scientifically underpinned and evidence-based analysis of the performance of the facial recognition algorithm currently used by MPS and SWP. Its findings revealed that there are settings at which the LFR algorithm can be operated with no statistically significant variation in performance between demographic groups.

The full results are presented in the NPL's commissioned report: Facial Recognition Technology in Law Enforcement Equitability Study[2]

The report found that when operating the LFR technology with a face-match threshold of 0.6, the variation in True Positive Identification Rate (i.e. the proportion of persons correctly identified against the watchlist) and False Positive Identification Rate (i.e. the proportion of persons not on the watchlist which return a false match against someone on the watchlist) was not statistically significant across gender and ethnicity.

The report also found that, when using a face-match threshold of 0.6, the LFR technology showed statistically significant variation between age groups for True Positive Identification Rate. The rate was 83% for under-20s, 89% for those aged 20 to 41, and 93% for those aged over 42.

The report recommended settings to be applied to the system in order to avoid any bias. *"Given our observations on the demographic variation in FPIR, we would recommend, where operationally possible, the use of a face-match of 0.6 or above to minimise the likelihood of any false positive and adverse impact on equitability."*

Immigration Enforcement will use a setting that exceeds the NPL recommended threshold and is the same as that applied by policing. This is set at 0.64. At this threshold, the report found that there were no false positive

[2] Facial Recognition Technology in Law Enforcement Equitability Study

identifications, leading to an equivalent FPIR of 0.0 for all demographic groups.

This EIA sets out IE's considerations regarding the impacts of using LFR technology in this context.

Section 2: Consideration of aim 1 of the duty: eliminate unlawful discrimination, harassment, victimisation, and any other conduct prohibited by the Equality Act 2010.

a. Direct discrimination

The use of LFR does not directly discriminate because it is not used to treat a person less favourably because of a protected characteristic. People passing through the Zone of Recognition are not subject to engagement or further action unless the system generates an alert and that alert is reviewed by trained staff.

IE deployments will only use LFR to locate individuals who meet the authorised, objective and pre-defined watchlist criteria for the specific deployment. Inclusion on a watchlist must be based on lawful, objective and pre-defined criteria, supported by a current immigration enforcement or criminal law enforcement purpose, and documented as necessary and proportionate. Individuals will not be included on a watchlist because of race, nationality, ethnicity, religion, sex, age, disability or any other protected characteristic.

b. Indirect discrimination

Consideration has been given to all protected characteristics and any potential areas of indirect discrimination.

Age

Risk of differential performance

The NPL report indicates that LFR has a higher true positive rate for older people when compared with people under 20. This means the system may be more likely to generate a correct alert for older watchlist subjects than for younger watchlist subjects.

In addition, the functionality, accuracy and performance of LFR may be less effective if a person's facial appearance has changed between the time the watchlist image was taken and the time the person enters the Zone of Recognition. The risk of a missed alert may increase where older images are used, particularly where the image was captured when the person was significantly younger.

Specific Mitigation

IE will mitigate the risk of age-related differential performance by operating the LFR system at the higher facial-match threshold of 0.64, consistent with the NPL findings. Alerts will not be treated as confirmation of a match or identity.

Each alert will be reviewed by a trained operator before any engagement is considered. Where an engagement is lawful and proportionate, engagement officers will carry out further identity checks before deciding whether any further operational action is required.

Watchlist images will be subject to quality assurance, including use of the most recent lawful image available and additional scrutiny where images are old or where age-related changes in appearance may reduce accuracy. Anyone under the age of 18 will not be included on the watchlist. IE will monitor deployment outcomes, including false alerts and confirmed matches by age band where lawful and proportionate, and will review or pause deployments if evidence indicates disproportionate impact on any age group. Findings will be considered through post-deployment review and used to refine threshold settings, watchlist criteria and officer guidance.

Disability

LFR alerts are based on mapping key facial indicators from an inputted image against the face of an individual entering or passing through a zone of recognition. Therefore, the functionality, accuracy and performance of LFR may be less effective if a person's facial appearance has changed between the time the watchlist image was taken and the time the subject enters the zone of recognition.

This may impact persons with facial disfigurement and/or facial structural changes through trauma, medical condition and/or intervention, or who are required to wear medical eyewear, and may mean that they are less likely to be flagged as a match. This could possibly be perceived as an advantage as they may be less likely to be matched and interviewed by an officer.
Those with visual disabilities and/or cognitive impairments may find it more difficult to read and understand signage which is designed to inform the person of the use of LFR.

Specific mitigations
Consideration has been given to:

- The camera angle and the LFR system's capability to template persons with genetic and/or medical conditions that impact on a person's height and/or wheelchair or mobility scooter users.
- The existence of any flashing lights that may affect persons with light sensitivity, visual impairment, and/or epilepsy.
- The accuracy of LFR system in relation to facial disfigurement as a result of injury/trauma and/or disability.
- Informing people who are partially sighted or visually impaired of the 'overt' use of LFR as they will be unable to 'view' the LFR signage.
- An officer will be located at the start of a zone of recognition and will be available to answer any questions or assist with any explanations and engage with members of the public.

Gender reassignment

Differential performance
LFR alerts are generated by comparing facial indicators from a watchlist image with a person entering or passing through a zone of recognition. Accuracy may be reduced where a person's facial appearance has changed due to gender reassignment since the watchlist image was taken. This creates a risk of differential performance where the image no longer reflects the person's current appearance. While this may reduce the likelihood of an alert, which could be seen as advantageous, it remains a potential equality impact because the system may operate less reliably for this group, leading to a risk of inconsistent treatment.

Specific mitigations
IE will mitigate this risk through pre-deployment watchlist quality assurance, including use of the most recent suitable and lawfully held image available and additional scrutiny where a person's appearance may have changed significantly since the image was taken. An alert will not be treated as confirmation of identity: every alert will be reviewed by a trained operator before any engagement is considered. Where an engagement is lawful and proportionate, engagement officers will carry out further identity checks before deciding whether any further operational action is required. Officers will be briefed to act respectfully, avoid assumptions based on a person's appearance or gender identity, and apply the same lawful, objective and proportionate decision-making standards in every case. Deployment outcomes, false alerts, complaints and equality concerns will be reviewed after deployment, and the deployment approach, watchlist image or officer guidance will be amended where evidence indicates a disproportionate impact.

Pregnancy and Maternity

The area of operation will be clearly signposted, and individuals will not be subject to additional intervention unless an alert is generated and reviewed by an officer.

However, pregnancy, recent childbirth, or travelling with young children may affect a person's ability to move comfortably through a busy or constrained Zone of Recognition, particularly where deployment equipment, signage, officers, passenger flow, luggage, prams or pushchairs reduce available space or require people to move more slowly.

Specific mitigations
Appropriate risk assessments and walkthroughs ahead of LFR deployments will take place to ensure the safety of all individuals moving through the Zone of Recognition.

In addition, signage will be present ahead of the LFR deployment to make people aware of the deployment in advance of entering the Zone of Recognition. IE officers will be on hand to provide support to those who require further assistance during LFR deployments.

Race (this encompasses, nationality, ethnicity, colour and national or ethnic origins)

Bias/differential performance: Concerns have been raised about LFR and racial bias, with some studies showing that there is a racial bias in the way LFR systems generate matches. It has been suggested that Black men are more likely to be incorrectly matched with watchlist individuals because of bias in algorithmic performance arising from available datasets. This issue was discussed in the *Bridges v SWP* [2020] EWCA Civ 1058 judgment.

To date, gender and ethnicity (and age) biases have received considerable attention, particularly from academics and government bodies. Relevant studies include Klare et al (2012), NIST (2018) and Buolamwini and Gebru (2018). The findings from Buolamwini and Gebru's study in particular were widely reported, as they found algorithms were particularly biased in terms of gender and ethnicity: performance was best for men and white individuals, and poor for women and black individuals.

The NPL's report in April 2023 found that at lower facial-match thresholds (0.58 and 0.56) the LFR technology *"starts to show a statistically significant imbalance between demographics with more Black subjects having a false positive than Asian or White subjects"*. It found at facial-match thresholds of 0.6 and 0.62 there was no statistically significant variation. At a facial-match threshold of 0.64 and above, there were no false positive identifications and accordingly no variance between racial groups.

The LFR deployments will use a facial-match threshold of 0.64, which the NPL report indicates will not lead to any race being placed at a particular disadvantage.

However, IE still needs to be alive to the risk that a facial recognition algorithm could perform differently across different racial/nationality groups.

Location of deployments: LFR may be deployed at a range of authorised locations across the UK, including ports, transport hubs, operational premises, joint operational settings or other locations where intelligence, threat, harm, operational necessity and proportionality support its use. The specific location, date, time, operational rationale and relevant authorised watchlist criteria will be clearly recorded in the Authorising Officer's documentation for each deployment.

Communication challenges: IE watchlists will consist of individuals who meet authorised, objective and pre-defined watchlist criteria for the specific deployment. Watchlists are generated from data which represents the diverse

multi-cultural modern world. Therefore, communication with individuals whose first language is not English may place them at a particular disadvantage.

Specific mitigations

Bias/differential performance: The LFR technology will be set at a facial-match threshold of 0.64. This reflects the NPL findings summarised above and is intended to reduce false positives and demographic variation.

Location of deployments: IE will mitigate the risk of particular nationalities or ethnic groups being placed at a disadvantage by ensuring deployments are intelligence-led, evidence-based and authorised for a specific operational purpose. Locations will not be selected because people present are likely to be of a particular nationality, ethnicity or race. Each deployment will have a documented rationale explaining why the location, date, time and authorised watchlist criteria are necessary and proportionate.

Communication and transparency: Clear and accessible signage will explain that LFR is in use, and officers will be available to answer questions about the technology. Any communication support required during a subsequent examination is governed by the guidance and arrangements applicable to the underlying operation.

To mitigate this and provide openness and transparency, IE will be conducting the following in the lead up to the use of the technology:

- A public-facing web page will be set up outlining the use of the technology along with the EIA and DPIA
- Where possible, and where it will not undermine the deployment's specific objectives, publish advance notice on Home Office websites at least 5 days before the deployment. The notice will explain the purpose of the deployment (for example, to help identify and locate people wanted for immigration offences).
- We will be using marked vehicles at any deployment site.
- Officers will be briefed ahead of any deployment and will be expected to explain the technology openly and clearly to any person who asks about it.
- We will clearly mark the zone and alert people via signs that they are approaching a facial recognition zone.
- Signage will be in English and Welsh (for deployments in Wales).
- Published content will be accessible, and members of the public will be able to use browser-based translation tools where available.

To support transparency, IE will refer to independent testing conducted by the National Institute of Standards and Technology (NIST), the National Physical Laboratory (NPL) and other relevant sources in documentation, including the EIA, DPIA and any public announcements. This will help reassure the public that facial recognition technology and its potential impacts have been subject to independent evaluation.

Religion or Belief

Religious facial coverings and headwear: The functionality, accuracy and performance of LFR may be less effective where a person's face is partially obstructed. Head or face coverings, facial hair and other items worn on or around the face are not limited to any religion or belief and may be worn for a range of personal, cultural, practical or medical reasons. However, such headwear or coverings may affect LFR effectiveness where they obscure facial features. While this may reduce the likelihood of an alert being generated, it may also create a disadvantage or perceived disadvantage if individuals who wear religious headwear or coverings feel they are being singled out or are subject to different treatment because of their appearance, religion or belief.

Religious beliefs and image capture: Some religions have sensitivities relating to photography or image capture. A lack of awareness or explanation about how LFR captures, processes and deletes images may therefore lead to concern, discontent or community tension, even where the deployment is overt and lawful. This could be viewed as a particular disadvantage.

Specific Mitigations

Religious facial coverings and headwear: Officers will be briefed that religious headwear, facial coverings, facial hair and other items worn on or around the face may be connected to religious observance and must not be treated as suspicious in themselves.

Religious beliefs and image capture: Where an individual raises concerns about image capture or religious sensitivity, officers will respond respectfully and provide a clear explanation of the legal basis, necessity, safeguards and deletion arrangements. Any concerns, complaints or community tension arising from deployment will be captured through post-deployment review and used to inform future engagement, signage, officer briefings and operational planning.

Sex

Differential performance: There may be some risk that LFR places a certain sex at a particular disadvantage because it produces a higher rate of false positive matches. This issue was discussed in the *Bridges v SWP* [2020] EWCA Civ 1058 judgment.

Earlier academic studies, including Klare et al. (2012), identified concerns that some facial recognition systems may perform less accurately for certain demographic groups, including Black women. More recent NPL testing of the specific system and threshold proposed for IE deployments found no statistically significant variation by gender or ethnicity at a 0.6 threshold and no false positives at 0.64. IE therefore treats this as a residual risk to be

monitored, rather than as evidence that the proposed deployment configuration will place women at a particular disadvantage.

However, IE still needs to be alive to the risk that a facial recognition algorithm could perform differently across different sexes.

Watchlisting: It is possible that some authorised watchlist categories may contain a higher proportion of men than women, reflecting underlying immigration enforcement and criminal justice data. This could lead to a greater proportion of men appearing on a watchlist for a particular deployment. This is not, in itself, considered to constitute a particular disadvantage and may simply reflect the individuals subject to immigration enforcement and/or criminal justice action. Nevertheless, it could be argued that it constitutes a particular disadvantage.

Specific mitigations

Differential performance: The LFR technology will be set to a facial-match threshold of 0.64. At this threshold, the NPL study reported no false positive identifications in its test data, resulting in an FPIR of 0.0 across the demographic groups tested.

Post-deployment review will consider false alerts, confirmed matches, equality concerns and any patterns that may indicate differential performance. Findings will inform future deployment planning, officer guidance and discussions with suppliers.

Watchlisting: IE will ensure that watchlist inclusion is based on lawful, objective and authorised watchlist criteria, not sex or any other protected characteristic. Any sex imbalance in a watchlist category will be considered as part of deployment planning, authorisation and post-deployment review.

Sexual Orientation

No particular disadvantage has been identified.

Marriage and Civil Partnership

No particular disadvantage has been identified.

General Mitigations

Individuals approaching or passing through the Zone of Recognition will be alerted to the fact that LFR is in use through clear and prominent signage. Where deployments take place in Wales, signage will be provided in English and Welsh. Officers will be clearly identifiable and available to answer

questions, provide reassurance and explain the use of the technology where appropriate.

IE will operate LFR with a threshold of 0.64, at which the NPL study found no statistically significant differences in demographic performance.

The use of LFR will be carefully monitored by Immigration Enforcement. The deployment will be subject to checks in line with College of Policing guidance. The Silver Commander must review the deployment at intervals set according to the deployment context and must record those reviews.

If an alert is generated, it will be reviewed by a trained operator before any engagement is considered. Where an engagement is lawful and proportionate, engagement officers will carry out further identity checks before deciding whether any further examination or operational action is required. Any subsequent action is governed by the powers, guidance and safeguards applicable to the underlying operation.

LFR supports officers in locating potential persons of interest, but it does not replace the officer's role in confirming whether the person is a match to the watchlist image or in making operational decisions. Officers use alerts as guidance, relying on their training before deciding whether to engage with someone. Any further action requires a lawful basis.

During deployments, LFR operators will be charged with actively monitoring performance. A contingency to halt the deployment will be in place in the event of poor performance during deployments.

Images and biometric data relating to people who do not generate an LFR alert are automatically and permanently deleted by the LFR system. CCTV footage is separate from LFR biometric processing.

Where CCTV is used as part of an IE-led or joint deployment, retention of CCTV footage will be managed under IE's or the applicable partner's CCTV, data protection, Criminal Procedure and Investigations Act 1996, complaints, conduct and operational record-keeping policies, as appropriate. CCTV footage should not be retained for longer than necessary and, where no longer required for a lawful purpose, will be deleted in accordance with the relevant retention schedule.

Justification

It is recognised that the use of LFR involves an interference with Article 8 ECHR rights, as identified in *Bridges*. IE has considered this interference when assessing whether the use of LFR is a proportionate means of achieving a legitimate aim.

IE considers that the use of LFR supports the legitimate aims of immigration control, border security, preventing and detecting crime, protecting the public, and safeguarding the integrity of the immigration system. The capability is

intended to help locate individuals who meet authorised, objective and pre-defined watchlist criteria for a specific deployment, where there is a current lawful immigration enforcement or criminal law enforcement purpose.

The interference is limited because LFR is not used against a broad or undefined population. For each deployment, the watchlist must be restricted to those who meet authorised criteria, and inclusion must be supported by a documented assessment of necessity and proportionality. Deployment location, date and time must also be justified by reference to intelligence, threat, harm, operational opportunity, expected footfall, public impact and relevant equality considerations.

LFR does not confirm identity or determine whether enforcement action should be taken. It generates a potential alert only. Any alert must be reviewed by trained officers, and any engagement or further action must be supported by lawful powers, further identity checks, safeguarding duties and case-specific necessity and proportionality.

LFR will be used only where other reasonable and less intrusive means of locating or identifying the relevant individuals have been considered and have either been unsuccessful or are not considered capable of achieving the deployment's lawful operational purpose effectively. This assessment will be documented as part of the necessity and proportionality case for each deployment.

IE considers that the use of LFR is proportionate because it is overt, targeted, time-limited, subject to senior authorisation, supported by clear signage and transparency measures, and governed by retention controls. Biometric data relating to people who do not generate an alert is automatically and permanently deleted. IE considers that, for the authorised deployment purposes described in this EIA, there is no less intrusive means of achieving the same operational outcome with equivalent effectiveness.

Section 3: Consideration of aim 2 of the duty: Advancing equality of opportunity between people who share a protected characteristic and people who do not share it.

The use of Live Facial Recognition by Immigration Enforcement is intended to help locate individuals who meet authorised watchlist criteria. It does not directly seek to improve or restrict access to opportunities, services or participation in public life for people with protected characteristics. However, IE recognises that equality of opportunity may be indirectly affected if any group experiences disproportionate false alerts, communication barriers, reduced understanding of signage, or reduced confidence in public authorities. These risks will be monitored through post-deployment review, complaints, officer observations and analysis of deployment data.

Section 4: Consideration of aim 3 of the duty: Fostering good relations between people who share a protected characteristic and persons who do not share it.

It is possible that Live Facial Recognition (LFR) may lead to some negative impact on groups that have a protected characteristic and those that do not, for example certain people could think they are being subject to LFR because of the action of others and feel resentment about this. This risk is considered to be modest given the limited impact on persons who are not matched or on the watchlist, with their biometric data being immediately deleted.

This risk may be mitigated as we plan to make the information publicly accessible, alongside overt signage when LFR is deployed, and we will encourage members of the public to view the system in use and to ask questions. We will also publish the outcomes of such operations.

Where deployments may affect communities with protected characteristics, IE will consider whether additional engagement, communications or reassurance activity is required before or after deployment. Feedback, complaints and community concerns will be reviewed as part of post-deployment governance. LFR deployments may also have a modest positive effect by increasing public confidence that IE is using proportionate, targeted and intelligence-led capabilities to locate individuals who meet authorised watchlist criteria.

These include persons subject to an extant Deportation Order, persons wanted on a warrant issued by a UK court in relation to an immigration-related offence, persons sought in relation to charges following a formal decision to seek their attendance or arrest, persons liable to detention under immigration legislation, persons currently and actively sought for enforcement and/or removal action by Immigration Officers, and persons who have failed to comply with immigration conditions of entry or stay or lawful removal directions.

The use of LFR aligns with wider objectives relating to controlled migration, irregular migration, public protection and the integrity of the immigration system.

Section 5: Ongoing compliance with the PSED.

When the LFR technology is deployed, IE will collect data recording details on the total number of faces processed during the deployment and the number that matched the watchlist.

Data captured in relation to watchlist matches during deployments will include quantitative information, such as the number of alerts, confirmed matches and false positives following officer review and further identity checks. This will contribute to IE continuing to assess the accuracy and effectiveness of the technology during deployments.

During deployment, the team may capture additional qualitative information about individuals engaged following an LFR alert, including relevant protected characteristic information where lawful, necessary and proportionate, to support compliance with the PSED.

Any collection or recording of protected characteristic information for monitoring purposes will be limited to what is lawful, necessary and proportionate, and will be handled in accordance with data protection requirements. IE will not require individuals to disclose protected characteristics.

IE will monitor equality impacts across different deployment types, locations and authorised watchlist categories to identify any emerging pattern of disproportionate impact. This will include review of alerts, confirmed matches, false alerts, complaints, officer observations and any equality concerns raised during or after deployment.

Findings will be considered through post-deployment review and relevant governance forums and will inform future authorisation, watchlist criteria, deployment planning, threshold settings, signage, briefing and officer guidance.

Section 6: Section 55 duty (for immigration, asylum, and nationality considerations only).

Children under the age of 18 will not be included on an LFR watchlist. The LFR-specific section 55 risk is that a child passing through the Zone of Recognition could be mistakenly selected as a potential match to an adult watchlist subject.

That risk will be mitigated through watchlist quality assurance, use of the most recent suitable and lawfully held image available, operation at the authorised threshold of 0.64 and trained operator review of every alert before any engagement is considered. Where an engagement is lawful and proportionate, engagement officers will carry out further identity checks before deciding whether any further action is required. An alert does not confirm identity and must not, by itself, determine whether a child or any other person is approached.

Any safeguarding consequence arising from subsequent engagement or operational action involving a child, parent, guardian or responsible adult is governed by the section 55 assessment, EIA, published guidance and authorising documentation applicable to the underlying CROP, STOP, Holyhead-type or other authorised operation, which must be read with this assessment.

Section 7: Risks to vulnerable individuals and other groups *(*if applicable).*

The LFR-specific risk for a vulnerable person is that facial changes, mobility needs, sensory or cognitive impairment, or difficulty understanding signage could affect system performance or awareness of the deployment. Mitigations include suitable camera positioning, accessible and prominent signage, officers available to explain the technology, trained operator review of every

alert before any engagement is considered, and further identity checks by engagement officers where an engagement is lawful and proportionate. Any vulnerability identified during subsequent engagement or operational action will be managed under the safeguarding guidance, EIA and authorisation applicable to the underlying operation.

Section 8: Declaration and sign off.

I have read the available evidence, and I am satisfied that this demonstrates compliance, where relevant, with section 149 of the Equality Act 2010 and that due regard has been had to the need to eliminate unlawful discrimination, advance equality of opportunity and foster good relations.

This EIA will be reviewed on: **07/09/27**

SCS Name & Title: Deputy Director, Immigration Compliance and Enforcement North

Directorate/Unit: Immigration Enforcement – Enforcement, Compliance & Crime

Lead contact: Emerging Technology Lead

Date: 07/09/26

Section 9: EIA Monitoring, Clearance and Publication.

Redacted

Section 10: Version Control

This document is subject to version control to ensure all updates, amendments, and reviews are accurately recorded and traceable. Each revision of the EIA will be assigned a version number and clearly dated. The version history will include details of changes made, the name of the individual responsible for the update, and confirmation of approval or sign-off by the relevant authority.

Version	Date	Description of Change	Author	Approved By
1.01	05/08/25	Final version		
1.02	03/10/25	Amended		

1.03	24/10/25	Updated		
1.04	18/02/26	Updated		
2.0	19/02/26	Final version 2		
2.1	06/07/26	Updated		Internal
2.2	20/08/26	Updated.		Internal
2.3	01/09/26	Updated		
2.4	07/09/26	Post SRO review		Internal

All subsequent changes must be logged in the table above to maintain a clear and auditable record of the document's evolution. This ensures transparency and facilitates effective monitoring and governance of the EIA process.