Home Office

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 intercept individuals of interest. Immigration Enforcement (IE) are looking to embrace this new technology as an effective means of managing those attempting to enter the UK in breach of a Deportation Order and those who are wanted for an immigration-related criminal offence but remain untraced through other more traditional methods.

LFR technology utilises biometric data to identify or locate individuals of interest. It does this by making a biometric comparison between subjects in the camera's field of vision and a preloaded database of persons who are of interest. The final decision as to whether the images are a match are made by an officer. The formal identification is done by trained officers after they have approached potential matches.

The technology employs a combination of hardware and software components. Cameras or other imaging devices capture the facial image, which is then processed by Computer Vision algorithms that analyse key facial landmarks, often referred to as a "faceprint" or "facial template."

Once the facial features are extracted, they are compared to a database containing pre-existing faceprints. The comparison is typically done using pattern recognition algorithms that measure the similarity between the captured facial image and the stored templates. Where there is no match, all data is immediately and permanently deleted

Despite its benefits, facial recognition technology raises concerns regarding privacy, accuracy, bias, and potential misuse. Privacy advocates warn of the risks associated with mass surveillance and the collection of sensitive biometric data without informed consent. For the proof-of-concept Immigration Enforcement will use images for the watchlist which 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]

It is of the upmost importance to the LFR team to address 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. This includes utilising existing data to highlight cohorts of individuals of high interest to IE to target exercises and ensuring clear signage during deployments to ensure public awareness and buy in to the exercise.

IE will only process the minimum amount of data in its use of LFR to target those who are entering in breach of a Deportation Order and those who are wanted for an immigration-related criminal offence. Where the LFR system does not generate an Alert then a person's biometric data is immediately automatically deleted. Where the LFR system generates an Alert, all personal data is deleted as soon as practicable and in any case within 24 hours. Where a false alert is generated, IE will look to retain anonymised demographic data to investigate any potential bias.

We will undertake a post-deployment debrief, review the results, and publish the number of individuals scanned, identified, and incorrectly identified.

LFR Deployments

Immigration Enforcement (IE) intend to use LFR as a precision tactic to locate people who are within IE's Population of Interest, specifically focussing on individuals who are entering in breach of a Deportation Order or who are wanted for an immigration-related criminal offence.

Deployments will look to match facial images from a pre-defined watchlist with those entering through a UK port using LFR. This will assist in the identification of people who are returning in breach of their Deportation Order, contrary to section 24(A1) of the Immigration Act 1971 or individuals who are wanted for an immigration-related criminal offence.

The purpose of overt operations are to intercept those people who may be Returning in Breach of a Deportation Order or who are wanted for an immigration-related criminal offence but remain at large, in a legally compliant and ethical manner to enable IE to achieve legitimate enforcement aims.

Deployment locations have been chosen specifically due to intelligence gathered on individuals returning in breach of deportation orders and using the Common Travel Area (CTA) to avoid detection by officials.

---

[1] Human Rights Act 1998

This presents a legitimate aim as outlined in Article 8(2) of the ECHR regarding the prevention of crime and national security. The use of LFR presents an opportunity to utilise existing technology to look at a range of people in order to locate those re-entering illegally by identifying those who are subject to a Deportation Order or individuals who are wanted for an immigration-related criminal offence. The use of the technology is proportionate as its focussed on a very small population of interest who are subject to a Deportation Order, and it further enhances officers' ability to ensure we have secure borders and to protect the UK.

Having an intelligence-led capability to actively look out for those that are subject to a Deportation Order or wanted for an immigration-related criminal offence ensures we are better able to maintain the integrity of the immigration system, prevents further criminal offending and protects the wider public and the security and safety of the UK. It is also anticipated that once the use of this technology is in the public domain it may have a deterrent effect as well further disrupting those who plan to abuse the system.

LFR Technical process

When two images are compared, the LFR system assigns a similarity score—a higher score means greater similarity. If this score exceeds a set threshold, the software generates an alert. Trained officers then review these alerts and decide on any necessary action. Thus, the LFR system supports the location of persons of interest, rather than replaces, human identification. The LFR will indicate a potential match to an officer, and after verifying that match the officer may speak to that person further to check their identity and ascertain if any offences have been committed. Where no offence is identified, the person will be free to continue their journey.

While facial recognition technology is generally assessed to be very accurate, leading to fewer misidentifications, it is important to acknowledge that "zero misidentifications" is not a realistic expectation. Even with high accuracy, there is always a possibility of wrongly identifying individuals, especially when dealing with different demographic groups and environmental factors. The technology is designed to focus on a specific population of interest but even then misidentification can occur.

The facial recognition technology and version of NEC Neoface V4, using HD5 Face Detector, is currently used by the Metropolitan Police Service (MPS), Sussex and Surrey Police (SSP) and South Wales Police (SWP) for Live Facial Recognition, Retrospective Facial Recognition and Operator Initiated Facial Recognition. This is the system used by an authorised LFR equipped police force and will be the one used for IE LFR deployments.

MPS and SWP tested Facial Recognition Technology (FRT) using this technology with the National Physical Laboratory (NPL).

The NPL is a world-leading centre of excellence that provides cutting-edge measurement in science, engineering and technology. Thanks to previous

testing by the National Institute of Standards and Technology (NIST) the MPS and SWP knew that their FRT used a high performing algorithm; the aim of the testing was to develop an in-depth understanding of the performance of the algorithms when it was being used in an 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 the MPS and SWP. Its findings revealed:

- there are settings at which the LFR algorithm can be operated at where there is no statistically significant variation between demographic performance.
- that there was no demographic performance variation for RFR; and
- that there was no demographic performance variation for OIFR

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 however did find that the LFR technology using a face-match threshold of 0.6 did have a statistically significant variation between age groups in respect of 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 the same setting as applied by Policing as we are using their equipment. This is set at 0.64.[3] At this threshold, the report

[2] Facial Recognition Technology in Law Enforcement Equitability Study
[3] Facial recognition Technology in Law Enforcement Equitability Study Para 1.4.5 page 5

found that there were no false positive identifications, leading to an equivalent FPIR of 0.0 for all demographic groups.

This EIA sets out the 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 – as it applies equally to all and does not treat a person less favourably because of a protected characteristic. Its use within IE deployments is set up to only look for those who are returning in breach of a Deportation Order or individuals who are wanted for an immigration-related criminal offence.

b. Indirect discrimination

Ahead of the pilot, 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 to under 20s. This may therefore place those cohorts at a particular disadvantage as they are more likely to be matched and examined by officers for the purpose of the trial.

In addition, the functionality, accuracy and performance of LFR may be less effective if changes to facial appearance have occurred between the time the Watchlist image was taken, and the time the subject enters the Zone of Recognition. The risk of a failure to match increases when facial images recorded at a young age are compared more than five years after they were collected. It accordingly may also place older cohorts at a particular disadvantage in that they are more likely to be matched.

Disability

LFR Alerts are based on the mapping of key facial indicators compared against an inputted face image to an individual's face entering or passing through a Zone of Recognition. Therefore, the functionality, accuracy and performance of LFR may be less effective if changes to facial appearance have occurred 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 changed through trauma, medical condition and/or intervention, or required to wear medical eyewear etc and 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 or 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 / mobility scooter users.
- The existence on 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 based on the mapping of key facial indicators when comparing an inputted face image to an individual's face entering or passing through a Zone of Recognition. Therefore, the functionality, accuracy and performance of LFR may be less effective if changes to facial appearance have occurred due to gender reassignment between the time the Watchlist image was taken, and the time the subject enters the Zone of Recognition. This presents a potential difference in treatment in that the system may not identify them based on previous images. This could possibly be perceived as an advantage as they may be less likely to be matched and interviewed by an officer.

Pregnancy and Maternity

The area of operation is clearly sign posted and an individual will not be subject to any additional intervention other than that they would usually experience during their journey. However, it is possible with additional equipment in place, pregnant individuals or those with young children may have trouble moving through the zone of recognition.

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 the LFR computer generates matches. It has been suggested that Black men are more likely to be incorrectly matched with watch list individuals because of bias in computer learning from available datasets. This issue was discussed in the *Bridges v SWP* [2020] EWCA Civ 1058 judgment, paragraphs 163 - 202.

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 National Physical Laboratory'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 a facial-match threshold of 0.6 and 0.62 there was no statistically significant variation. At facial-match threshold of 0.64 and above, there was no false positive identifications and accordingly no variance between racial groups. The LFR proof of concept 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: We are utilising LFR technology in a UK port. This port primarily services passenger from Dublin meaning all passengers are within the Common Travel Area (CTA) both upon alighting and disembarking the ferry. Most passengers are either UK or Irish nationals, with some international tourists using the route as part of broader travel across the British Isles. Such nationalities could therefore possibly argue that they are placed at a particular disadvantage by the location of deployments.

Communication challenges: IE's population of interest and watchlists generated from 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 is set at a facial-match threshold of 0.64. This threshold has been shown to significantly reduce the number of false positives, including leading to much lower variation in demographic difference, which the NPL report describes as not being statistically significant.

Communication challenges: IE will not be able to accommodate all languages during deployments through translation of signage or in person translation. IE officers will communicate with individuals in a respectful manner and where necessary can use the services of telephone interpreters. Further intervention or conversations with individuals can be conducted in a separate location for the duration of the deployment.

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
- We will publish ahead of any planned deployments the dates of the use of the technology.
- We will be using marked vehicles at any deployment site.
- Officers will be briefed ahead of any deployment and will be informed to be open and explain with any person interested in the technology.
- 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).
- It is not practical or reasonable to produce documentation in every language. However, anyone who is stopped will be spoken to and an explanation given. This task will be carried out with the assistance of an on-call translator when necessary. Additionally, it is common practice in our work to utilise interpreters and/or translators as needed, and we can provide phone translation services if required.
- The Media content we plan on publishing will be accessible by all and people will be able to utilise any translation software provided by their web browser (e.g. Google Translate).

To ensure transparency, we will provide a reference to the independent testing conducted by the National Institute of Standards & Technology (NIST), National Physical Laboratory (NPL) and other relevant sources in our documentation. This will include citations within the EIA, DPIA, and any public announcements. By citing these sources, we aim to reassure the public of the

thorough evaluations conducted on facial recognition technology and its potential impacts.

Religion or Belief

Religious Head Coverings: The functionality, accuracy and performance of LFR may be less effective if the face is obstructed. Items adorned on the head and/or face are not limited to a particular religion or belief (and can be a style decision, or a decision by necessity, by any member of the community). Nevertheless, the wearing of religious headwear/ coverings and/or facial hair may have a bearing on LFR effectiveness. Again, this could be viewed as an advantage to the individual as it may mean that they are less likely to be matched.

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, paragraphs 163 - 202.

Academic studies have indicated that LFR performance is worst for black women: Klare et al (2012). Social observation indicates women change their appearance more frequently and significantly than men which may impact the performance of LFR. Reports suggest that facial contouring through the use of cosmetic make-up application may impact on the LFR system's performance.

The NPL report found that with a facial-match threshold of 0.6, that there was no statistically significant variation between genders in the True Positive Identification Rate. It also found that there was at a facial-match threshold of 0.64, which this proof of concept will use, there was no false positives, meaning no variation between the sexes. The report indicates that the IE approach will not place any sex 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.

Watch listing: It is understood that more men than women have been subject to deportation action or are wanted for immigration-related criminal offences, and that they will therefore form a majority of the images on the watchlist. They could therefore possibly seek to argue that they are placed at a particular disadvantage by the LFR pilot.

Specific mitigations

The LFR technology will be set to a facial-match threshold of 0.64. This threshold has been shown to significantly reduce the number of false positives, including leading to much lower variation in demographic performance.

The post-Deployment review process is used to examine False Alerts and determine if there is trend or overriding cause. Data will be stored on the effectiveness of the pilot and fed into IE LFR forums for discussion. Informing further discussion with LFR providers to increase performance.

Sexual Orientation

No particular disadvantage has been identified.

Marriage and Civil Partnership

No particular disadvantage has been identified.

General Mitigations

Passengers arriving will be alerted to the fact LFR is in use and we will be doing this via bilingual English and Welsh signs (if deployment takes place in Wales). This will be prominently displayed along the route to the arrivals hall and officers will be clearly identifiable and passengers will have the opportunity to speak with officers if they have any questions.

The use of LFR will be carefully monitored by Immigration Enforcement. The deployment of the system will have gone through a number of checks in line with College of Policing guidance. The system will be activated, and the deployment will be reviewed every two hours to confirm its necessity and system accuracy.

In the event an alert is generated officer will review it assess whether it is a correct match. Only if the officer is so satisfied, will the passenger then be approached and the reason for the stop explained to them, and they will be provided with an information leaflet. Officers also have access to interpreters and can speak with people via this to explain the system if English or Welsh are not their first language.

It is important to underline that LFR supports officers locating potential persons of interest, but it does not usurp the officer's function to confirm they are satisfied that the person of interest is a match to the watchlist image or to make decisions itself. Officers use Alerts as guidance, relying on their training before deciding to engage with someone. Even if officers engage, 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.

The post-deployment review process is used to examine False Alerts and determine if there is trend or overriding cause. Data will be stored on the effectiveness of the pilot and fed into IE LFR forums for discussion. Informing further discussion with LFR providers to increase performance.

Justification

It is recognised that there is a privacy interference under Article 8 ECHR in the use of LFR: *Bridges*. We have taken this factor into account in assessing whether the use of this technology is a proportionate means of achieving a legitimate aim.

Considering the above mitigations, we consider the LFR is a proportionate means of achieving the legitimate aims of supporting immigration/border control and detecting and investigating crime.

There is intelligence and previous outcomes indicating that Common Travel Area (CTA) and domestic UK mainland routes are being exploited by immigration offenders attempting to enter or exit the UK undetected or to circumvent border controls. Border Officers do not routinely conduct immigration checks at CTA ports.

UK authorities are permitted to undertake necessary activities to identify individuals who require permission to enter the country including when they are entering via a local CTA journey. This includes those subject to a deportation order: see section 9(4) of the Immigration Act 1971. Part 3 of the Immigration Act 1971 sets out a number of criminal offences and includes powers to obtain a warrant in respect of the investigation and prosecution of such offences. The watchlist used by the LFR system is limited to individuals subject to extant deportation orders issued by the UK and those who are wanted for an immigration-related criminal offence. This targeted approach helps minimise the risk of collateral intrusion.

Images/biometric data of those who don't cause an alert are automatically and immediately deleted (0.5 seconds). CCTV footage is separate to the LFR. If CCTV is used as part of the deployment, then all CCTV footage generated from a mobile CCTV deployment is deleted within 31 days, except in the following examples when it is retained:

- in accordance with the Data Protection Act 2018, MOPI and the Criminal Procedures and Investigations Act 1996; and /or
- in accordance with Immigration Enforcements complaints / conduct investigation policies.

Importantly, the LFR system does not confirm the commission of an offence or need for engagement. It merely indicates that a person may be subject to a deportation order or is a person who is wanted for an immigration-related criminal offence. It is then the responsibility of an Immigration Officer to review the purported match and engage with the individual and determine whether any offences have occurred or already been committed. The final decision rests solely with the officer.

Use of LFR if considered to be proportionate as it supports the identification of persons returning in breach of a deportation order or individuals who are wanted for an immigration-related criminal offence. It means that there is clear intelligence (i.e. the system flagging the match, and an officer confirming they are satisfied that there is a match, giving further confidence in the underlying

data quality) before a person is engaged with. It has limited impact on persons who are not of interest as their image is immediately deleted, and they are not subject to any delays in respect of their journey. It also respects the Immigration Act 1971 in that there are no general immigration controls on local CTA journeys and means that officers are able to target their resource at key border issues (i.e. persons returning in breach of a deportation order or seeking to avoid detection by officials due to their past criminal conduct).

There is a risk to the security and safety of the UK border controls by not responding to these issues. There is interference with people's privacy rights by using LFR however the intrusion must be balanced against the above point around border security and the prevention and detection of crime, and it is deemed proportionate to infringe the privacy of passengers in this way, as there is no other way of achieving the same outcome without more significant intrusions. Passengers will be made aware of the use of LFR through posters, a website and officers at the port.

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 LFR deployments are not considered to substantively affect this limb of the PSED.

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.

This risk may be mitigated as we have a reactive media strategy in place in respect of LFR deployments. We have planned on making the information publicly accessible as well as overt signage when the van 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.

LFR deployments may also have a modest positive effect by increasing public confidence that persons seeking to return in breach of a deportation order or who are wanted for an immigration-related criminal offence are being identified. The actions of the pilot align with current governmental targets regarding both controlled migration and irregular migration and therefore could be seen as a positive step towards this.

Section 5: Ongoing compliance with the PSED.

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

Data captured on those who match the watchlist during the deployments will consist of both quantitative data such as the number of matches to the watchlist, compared to false positives fallowing second line intervention and further identity checks. This then gives the team data on the accuracy and effectiveness of the technology during the pilot.

Border Force already routinely check passenger manifests from ships arriving into the UK from Ireland and respond accordingly by reacting to any identified persons of interest by bolstering the control.

During the deployment, the team will capture additional qualitative data on those intercepted by the LFR technology in terms of recording details on protected characteristics to support compliance with the PSED.

Data collated on deployments will be published for transparency with the public. This data will consist only of quantitative data limited to numbers entering the zone of recognition, matches to the watchlists and details on further arrests based on the intelligence. No data linked to protected characteristics or personal details will be published.

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

The need to safeguard and promote the welfare of children in the UK has been considered. Any current watchlist criteria will preclude minors. Generally, minors will not be subject to a deportation order and/or wanted for immigration-related offences. For example, minors are excluded from the effect of the auto-deportation regime in section 32 of the UK Borders Act 2007. However, children's parents and/or legal guardians may be subject to a deportation order. We recognise that refusing entry to the United Kingdom or detaining individuals who are parents/guardians of children for returning in breach of deportation orders, or in relation to immigration-related criminal offences, may have an impact on the lives of children, particularly if the children then need to leave the UK to remain with their parents.

However, it is noted that to issue a deportation order full consideration of the impacts on children under section 55 will have been given. Intelligence gathered on individuals circumventing this control through the Common Travel Area justifies the use of this technology and any impacts thereof.

The section 55 duty will of course be considered in individual cases where a parent/guardian may be subject to arrest for immigration-related criminal offences or in any decision to refuse entry to a parent/guardian from the UK or to remove them from the UK.

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

This proposal may have an impact on vulnerable groups. Due care is taken in issuing deportation orders to comply with legislation to protect individuals. There aren't any measures in place to monitor individual's personal circumstances post-deportation as this may impeach on a person's right to privacy.

Therefore, there may be cases where an individual, in the time since they were removed from the UK, is now classed as vulnerable. In this instance further due care must be taken to prevent further harm to the individual while relevant action is conducted.

IE officers will be in attendance for the duration of the pilot. Officers have received comprehensive training in handling individuals with a wide range of needs and vulnerabilities. Therefore, the immediate handling of individuals with vulnerabilities is well practiced amongst this group and further steps to protect those who present with vulnerabilities will be in place.

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: **01/08/2026**

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

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

Lead contact: M. Wilkinson, Emerging Technology Lead

Date: 18/02/2026

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	M Wilkinson	G Summers
1.02	03/10/25	Amended	M Wilkinson	G Summers
1.03	24/10/25	Updated	M Wilkinson	G Summers
1.04	18/02/26	Updated	M Wilkinson	G Summers
2.0	19/02/26	Final version 2	M Wilkinson	R Cage

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.