The first phase of Australia’s new biometric Face Verification Service (FVS) is now operational, providing the Department of Foreign Affairs and Trade and the Australian Federal Police access to visa and citizenship images held by the Department of Immigration and Border Protection (DIBP).

Other types of images such as passport and driver licence photos will be added over time, with access expanded to other government agencies. In addition, a Face Identification Service (FIS) is expected to commence in 2017 to determine the identity of unknown persons.

The Attorney-General’s Department manages the system, on behalf of participating agencies, which will be operated along similar lines to the Document Verification Service (DVS).

What is the FVS?

The FVS is a one-to-one image based verification service that can match a person’s photo against an image on one of their government records, such as a passport photo, to verify their identity. Often these transactions will occur with the individual’s consent.

For example, where a person uses their citizenship record as evidence of their identity to apply for a passport, the system could enable the passport office to ask DIBP to confirm the identity of the passport applicant.

What is the FIS?

The FIS is a one-to-many image based identification service that can match a photo of an unknown person against multiple government records to help establish their identity. Access to the FIS will be limited to police and security agencies, or specialist fraud prevention areas within agencies that issue passports, and immigration and citizenship documents.

Police will only be able to use the FIS for investigations of more serious offences. For example, it may be used to identify a suspected paedophile from child exploitation material, or to identify an armed robber from a still image taken from CCTV footage. It will not be used for minor offences such as littering or parking infringements.

Access to the FIS will only be provided to a limited number of users in specialist areas with training in how to interpret the results, to help guard against the potential for false matches.

Why are these face matching services necessary?

The Australian Government is investing in this new system to help combat identity crime, which is one of the most common crimes in Australia and costs around $2.2 billion per year. Around 1 in 20 Australians experience identity crime each year that results in financial loss.
Identity crime is a key enabler of serious and organised crime, such as drug trafficking, money laundering, people smuggling, child exploitation and terrorism. Australians convicted of terrorism offences have used false names to avoid detection while planning attacks. This includes purchasing ammunition and chemicals to make explosives and pre-paid mobile phones to communicate anonymously.

While existing measures such as the DVS are helping to prevent the use of fake identity documents, criminals are now producing high quality fraudulent identity documents. These documents contain personal information stolen from innocent and unknowing victims, but with someone else’s photo – documents that would pass a DVS check.

Preventing this type of fraud can be assisted by greater use of biometrics, such as the FVS and FIS.

The use of face matching services will help agencies:

- protect people from identity theft, and help victims restore their compromised identities
- prevent criminals and terrorists creating and using fraudulent identity documents, and
- investigate other serious criminal activity.

What security and privacy protections has the government put in place?

The system is not a new centralised biometric database, but a secure means of sharing images between existing agency systems. The central infrastructure will exchange messages but it will not conduct any matching nor store any personal information. This approach allows individual agencies to retain full control over their own image holdings and decisions about the organisations with which they share this information.

Participating agencies will require a lawful basis to collect and use facial images, just as they do now. For example, the Commonwealth Privacy Act 1988 permits the Australian Federal Police to collect, use and disclose facial images where it is reasonably necessary to fulfil its enforcement functions.

Commonwealth legislation relating to passports, immigration and citizenship documents enables personal information to be shared with certain agencies where it is reasonably necessary for enforcement purposes. Most states and territories will need to amend legislation to enable road agencies, which issue driver licences, to participate in the system.

The system will have robust privacy safeguards, informed by independent privacy impact assessments conducted throughout the design and implementation phases, in consultation with the Australian Privacy Commissioner. These assessments will be published wherever possible, so that the community can see the safeguards that are being built into the system.

Participating agencies will also need to enter formal data sharing agreements containing safeguards for the sharing and use of personal information. These agencies are already subject to audits and independent oversight by a range of existing external bodies such as privacy commissioners, ombudsmen and anti-corruption or integrity commissioners for their use of personal information. This will continue when they use the services.

The system will adopt best practice security and access arrangements in accordance with the Protective Security Policy Framework and the Information Security Manual.