National Identity Security Strategy

A National Biometric Interoperability Framework for Government in Australia

IDENTITY SECURITY

Preamble

The 2012 National Identity Security Strategy (NISS) identifies the development of a National Biometric Interoperability Framework (the Framework) as an implementation goal. This Framework aims to ensure a coherent and consistent approach to the collection, use, disclosure and management of biometrics across the Commonwealth and state and territory governments (Australian governments).

Enhancing the interoperability of biometric systems can significantly assist in addressing national security and criminal threats and offer new opportunities for enhanced service delivery. These benefits will be realised through greater opportunities for the lawful sharing of biometric information and biometric capabilities between governments and greater collaboration on biometric system development.

The Framework works within existing legislation, including privacy legislation, and promotes the highest standards of protection for biometric uses. The Framework also improves Australians confidence in government by providing transparent and accessible avenues for redress by the public. It also encourages the employment of appropriate safeguards for the use of personal information, when collecting and sharing biometrics.

Background

Biometric systems are currently used by a range of government agencies in Australia to establish and verify a person's identity with greater accuracy. This has increased benefits for national security, law enforcement, border management and service delivery outcomes. As the cost of biometric technologies decrease, and the availability of software applications increase, the range of agencies seeking to develop biometric systems, and the uses to which these systems can be applied, will continue to expand.

In many cases, biometric systems work within individual agencies, producing a range of security and facilitation benefits. The utility of biometric systems can be enhanced through the ability, where reasonably necessary, to share biometric data between agencies and to verify data against other agency holdings. Enhancing the interoperability of biometric systems between government agencies in Australia has a range of potential benefits, including:

- improving Australians' identity security by establishing unique identity records that are more stable, more durable and less susceptible to interference or duplication that those based on biographical or other forms of personal information;
- combating criminal and other national security threats by enhancing the ability of law enforcement agencies to identify persons of interest;
- facilitating greater online service delivery by providing agencies with increased confidence in enrolment and authentication processes; and
- generating operational or cost efficiencies through sharing information and expertise in the development and implementation of biometric systems, including in developing standards, systems evaluation, capability development and joint procurement.

While there are opportunities to enhance the interoperability of biometric systems in achieving these aims, these need to be balanced against the need for appropriate privacy and other safeguards. This is in order to give the community confidence that personal information contained in biometrics will be adequately protected and handled in accordance with the law.

Guiding Principles

Below are a set of proposed principles underpinning biometric interoperability that form the basis of the Framework:

1. Biometric Types and Data Integrity

Government agencies in Australia should, where possible, consider adopting fingerprints and facial scans as biometric types of preference. Other biometrics may become preferred for particular uses in time and the Framework provides a basis to manage the related interoperability objectives.

The choice of biometric should involve considering the most appropriate and cost-effective means of achieving agency business needs, through a comprehensive cost-benefit analysis, including any impact on the privacy of consumers and security risks involved in collecting and holding such information. The use of biometrics should apply high standards, both in identity verification and in maintaining biometric data integrity, recognising that the effectiveness of biometrics depends on the integrity of agency systems.

2. Systems and Standards

All collectors and users of biometric data should work to agreed standards, with the Centres of Expertise responsible for identifying 'best practice' and producing appropriate guidance for particular biometric types or biometric applications that would assist in achieving biometric interoperability across Australian Governments.

3. Sharing

Where authorised and subject to law and privacy requirements, biometric data should be capable of being shared amongst government agencies in Australia and received from private sector organisations.

4. Security

Biometric systems should be supported by high levels of security to guard against unauthorised or unintended release or access of biometric data and to maintain data integrity.

5. Communications

Government agencies in Australia that use biometric data should communicate with clients and the general public to promote understanding about the use of biometrics and public confidence in those agencies' collection, use, disclosure and management of biometrics.

6. Centres of Expertise (COEs)

Government agencies in Australia can assist the operation of COEs by facilitating the nomination and appointment of government agency representatives who will share knowledge and raise awareness about biometrics. These COEs will develop and promote best practice and standardisation for a particular biometric technology, thereby achieving interoperability.

7. Procurement

Government agencies in Australia should factor design for interoperability into business processes and Information and Communications Technology refresh cycles. Government agencies should also consider the ease with which systems interact with others, and work towards 'future proofing'.

8. Privacy

Government agencies in Australia should expressly recognise and consider the role of privacy when engaging in the collection, use, disclosure, management and disposal of biometric data.

Implementation

The biometric Centre's of Expertise (COEs) will be the primary vehicles for implementation of the Framework. The agencies of Australian governments can participate in the Facial and/or Fingerprint COEs operating on a national basis. Each COE will involve those agencies with expertise in the use of that technology.

The COEs have the aims of:

- examining the suitability of relevant standards that would support interoperability and identify areas for further work, with a particular focus on collection, storage, authentication, and sharing of biometric information;
- identifying the current capability development activities and develop cooperative approaches to these; and
- identifying opportunities for cooperation in the management of current operationally deployed biometric systems.

Implementation of the Framework will be staged over time, recognising the individual circumstances of each government in Australia and needs of individual government agencies. Initially, implementation would be through collaborative work within and between Australian governments on procedures and standards for interoperability.

Governance

The National Identity Security Coordination Group (NISCG) shall be the governing body of the Framework. The NISCG's role as the governing body for the Framework involves encouraging:

- Australian governments agencies to adopt the Framework and undertake activities in accordance with the principles underpinning the Framework
- Australian governments agencies to participate in the activities of the COEs, including COE work plans and pilot projects, and
- the adoption of relevant interoperability standards and procedures that will support work in achieving the principles of the Framework.