Impact Summary: Improvements to the accuracy and timeliness of Police information regarding name changes, deaths and non-disclosure directions

Section 1: General information

Purpose
New Zealand Police (Police) is solely responsible for the analysis and advice set out in this Regulatory Impact Statement. Police has worked closely with the Department of Internal Affairs (DIA) to develop this advice. The core purpose of the proposed Approved Information Sharing Agreement (AISA) is to improve the accuracy of Police information regarding names, vital status, and active non-disclosure directions.
Key Limitations or Constraints on Analysis
The proposed AISA is a part of the wider work programme to respond to the Government Inquiry into the Escape of Phillip Smith/Traynor. The Cabinet of the previous Government agreed that an AISA be developed to enable the Registrar-General to regularly share death and name change information with Police [CAB-17-Min-0414]. In October 2018, Cabinet agreed that the draft AISA be released for public consultation [CAB-18-MIN-0484]. The Privacy Act 1993 sets the framework for what an AISA can contain and the issues it can address, such as authorising exemptions from any of the information privacy principles. The Act also sets out the process that must be followed to make an AISA. The Births, Deaths, Marriages, and Relationships Registration Act 1995 enables certain personal information to be shared by the Registrar-General under an AISA. To come into force, an AISA must be created by Order in Council and its operation is subject to review by the Privacy Commissioner.
Responsible Manager (signature and date):
Gillian Ferguson Acting Director, Policy & Partnerships New Zealand Police 18 April 2019

Section 2: Problem definition and objectives

2.1 What is the policy problem or opportunity?

Background

In December 2014, the Government Inquiry into the Escape of Phillip Smith/Traynor (the Inquiry) was established following the illegal departure from New Zealand of a prisoner on temporary release. The Inquiry exposed limitations with identity management practices and systems in the criminal justice sector. It made a suite of recommendations, including how relevant agencies could better manage identity information across the justice sector.

A significant amount of business, operational, and legislative reforms have been implemented in response to the Inquiry recommendations. The recent justice sector identity management focus has been on improving the connections between key agencies' information systems and how agencies share information. This has included a project to enrich the quality of the information used by Police to more accurately identify individuals – the Progressive Steps Project.

Progressive Steps has resulted in Police being able to access driver licence photos from the NZ Transport Agency and access identity information on non-New Zealanders held by Immigration New Zealand. Two other initiatives are under development as part of Progressive Steps. The first, expected to be implemented by mid-2019, will enable Police to access certain birth and passport information held by the Department of Internal Affairs (DIA). The other initiative, which is the subject of this Impact Statement, is to enable the Registrar-General to proactively provide Police with information regarding registered deaths, registered name changes, and non-disclosure directions. A non-disclosure direction restricts public access to records to protect the safety of a person, but does not limit information being shared with Police under an AISA.

The problem/opportunity

Police is not aware, as a matter of course, if people change their name, die, or obtain non-disclosure directions. Police is sometimes informed of such information during the ordinary course of Police business. In these cases Police can update identity information held about people in Police's National Intelligence Application (NIA) on a case-by-case basis (e.g. when interviewing a person who has changed their name, or when investigating a suspicious death). However, information about all registered name changes, registered deaths, or non-disclosure directions is not systematically passed on to Police by the Registrar-General.

This impacts on the accuracy and completeness of the identity information Police holds in NIA, which is the information system that contains the information necessary to support Police's ability to maintain the law.

There are around 6,000 to 7,000 name changes per year and approximately 30,000 death notifications per year. There are currently around 95 non-disclosure directions in force. These figures provide a 'ball park' indicator of the size of the information gap. However, while not all of these people will already be in NIA, NIA does have over 5 million records.

Even if only a proportion of those who change their name, die or obtain a non-disclosure direction each year are in NIA, then there will still likely be hundreds of matches and updates that could be made each year.

Inaccurate or incomplete information can impact on Police being able to efficiently and

effectively provide public services (including the maintenance and enforcement of the law).

Inaccurate/incomplete information can result in a number of undesirable scenarios:

- An individual may change their name on the birth register and apply for a passport in their new name. Unless Police knows of the name change, Police cannot ensure that any border alert against the person has the new name added. The person may therefore be able to evade the border alert and travel overseas.

- If Police does not know that a firearms licence holder has died, then Police cannot update the firearms licence database and follow-up to ensure any firearms the licensee may have held are transferred to another licence holder or disposed of. Better information may support the wider work programme on strengthening the regulatory regime for firearms.

- If Police does not know that a person with an active warrant for their arrest has died then Police cannot revoke the warrant. This could result in Police seeking to execute the warrant, wasting time and resources, and potentially upsetting the family of the deceased person.

- If Police is not notified that an individual has a non-disclosure direction in place to ensure that their new name is not accessible to the public, then they could inadvertently disclose the person's new name – e.g. when interviewing a person in response to a complaint by the person who had changed their name.

Inaccurate identity information on Police's system can then feed inaccurate information into the criminal justice system including the courts and corrections services.

Existing legislation

Currently, Police can request the Registrar-General to disclose certain identity information about an individual. This includes whether the person in question has changed their name or died. However, under section 78AB of the Births, Deaths, Marriages, and Relationships Registration Act 1995 (BDMRR Act) such requests can only be made on a case-by-case basis, in specific circumstances. To request such information, Police must have a reason to suspect that the particular individual:

- is, or is liable to be, detained under an enactment
- is, or is liable to be, arrested under a warrant issued by a court or any Registrar
- is contravening, or is about to contravene, an enactment or a court order
- is liable to be prosecuted for an offence punishable by imprisonment
- is, or is liable to be, detained or arrested in respect of a traffic offence
- is endangering, or is threatening to endanger, the life, health, or safety of a person or group of persons
- is injured or dead.

This mechanism enables Police to obtain the information in specific circumstances for particular individuals. Police either needs to be actively dealing with the person or needs to be aware that there might be a change in the first place. Currently, information is being 'pulled' by Police if Police make specific queries for it on a case-by-case basis. It is not being proactively and systematically 'pushed' to Police by the Registrar-General in bulk, regular transfers. As noted above, Police requires the information because it is not aware of the majority of cases where a person has changed their name, died, or has a non-disclosure direction in force.

2.2 Who is affected and how?

The core purpose of the proposed AISA is to enable the sharing of information between two government agencies to provide better public services (in this case law enforcement).

The main parties directly impacted are DIA and Police who have had to develop the AISA and the supporting IT system to enable the sharing of such information.

Other parties impacted include anyone who changes their name, dies, or obtains a non-disclosure direction. It is (a subset of) their personal information collected by the Registrar-General that will be provided to Police – although in reality this transfer will happen automatically without any direct impact on the people concerned.

While the proposal involves sharing of personal information, it has been developed within the Privacy Act's framework, which was established to enable such information sharing for legitimate purposes and to ensure appropriate privacy safeguards are applied.

No significant opposition to the proposed AISA was provided during public consultation (see section 5, below), or is expected if the proposed AISA is approved.

2.3 Are there any constraints on the scope for decision making?

As noted in section 1, the previous Cabinet agreed that an AISA be developed to enable the Registrar-General to regularly share death and name change information with Police [CAB-17-Min-0414].

In October 2018, the current Cabinet agreed that the draft AISA (which also included sharing on non-disclosure directions) be released for public consultation [CAB-18-MIN-0484].

The proposal is one of a series of complementary initiatives being implemented as part of the Progressive Steps Project that was initiated in response to the Smith/Traynor Inquiry (see section 2.1, above).

Section 3: Options identification

3.1 What options have been considered?

The overarching objective is for Police to have accurate and up-to-date information.

The criteria used to consider the options included:

(a) **Effectiveness.** The preferred option needs to improve the accuracy of the identity information held by Police in NIA regarding registered name changes, registered deaths, and non-disclosure directions. More accurate information will support Police to maintain the law and provide public services.

(b) **Efficiency**. The preferred option needs to provide for the ongoing proactive, efficient, and regular provision of such information by the Registrar-General to Police to ensure the accuracy of the identity information in NIA is maintained and enhanced over time.

(c) **Privacy.** The preferred option needs to provide for appropriate protection of individuals' privacy and ensure a proper level of security and transparency when sharing such information.

(d) **Administrative efficiency**. The development of the preferred option needs to be administratively efficient (including in terms of timeliness, longevity and cost).

Criterion (a) to (c) are weighted evenly, with less weight given to criteria (d) (due to it mainly relating to the immediate mechanism to enable the sharing of information).

The following options were considered:

- Option 1: Retain the status quo
- Option 2: Police and the Registrar-General sign a Memorandum Of Understanding (MOU) to share information
- Option 3: Police and the Registrar-General agree to an Approved Information Sharing Agreement (AISA)
- Options 4(a)-(c): Other legislative mechanisms:
  - (a) adding Police to Schedule 1A of the BDMRRA
  - (b) Using Part 10A of the Privacy Act
  - (c) Bespoke legislative change.

<u>Option 1: retain the status quo</u>

Description

As discussed at section 2.1 above, under the BDMRR Act Police can request the Registrar-General to disclose identity information about particular individuals on a case-by-case basis in specific circumstances. Police either needs to be actively dealing with the person or needs to be aware that there might be a change in the first place. However, Police is not aware of the majority of cases where a person has changed their name, died, or has a non-disclosure direction in force.

Analysis

If the sharing continues to be based on individual queries from Police then most updated name change, death, and non-disclosure direction information about a person in NIA will not become known to Police in a timely manner. The current issue of inaccurate identity information on Police's system, which then feeds inaccurate information into the criminal justice system, would not be addressed.

The status quo therefore only partially meets the effectiveness criteria (a) and does not meet the efficiency criteria (b). The privacy criteria (c) continues to be met, and the administrative efficiency criteria (d) is met by default (as no further development beyond the status quo is required).

Option 2: Police and the Registrar-General sign a MOU to share information

Description

A Memorandum of Understanding could be drawn up between Police and the Registrar-General.

Analysis

This would have the same issues as the above option, as information sharing would be based on specific queries and not received proactively in bulk. Therefore option 2 only partially meets the effectiveness criteria (a) and does not meet the efficiency criteria (b). A MOU could meet the privacy criteria (c) and the administrative efficiency criteria (d).

Option 3: Police and the Registrar-General agree to an Approved Information Sharing Agreement (AISA)

Option 3 is the preferred option, and is discussed in detail at section 3.2 below.

Option 4(a) – Using section 78A of the BDMRRA – Information Matching Agreement

Description

Section 78A of the BDMRRA provides a mechanism to authorise the disclosure of birth, death, marriage, civil union, and name change information to certain specified agencies for certain purposes utilising an Information Matching Agreement (IMA).

Police would need to be added to Schedule 1A of the BDMRRA, along with the type of information to be disclosed, and the specific purpose for disclosing the information. An IMA could then be developed in accordance with s78A.

Analysis

While this mechanism could provide a way of enabling the proposed sharing of information, it is not supported. Change to primary legislation is not actually necessary and is counter to the intent of establishing the AISA framework in the Privacy Act in the first place.

Additionally, in the broader legislative context, the Privacy Bill currently before the House proposes that the development of new information matching agreements be discontinued, and that future information sharing be authorised through AISAs. If passed, the Schedule 1A mechanism will cease to be changed to extend information sharing and in the longer term it will likely be removed.

While this option could meet the effectiveness criteria (a), the efficiency criteria (b) and the privacy criteria (c), it does not meet the administrative efficiency criteria (d). The administrative cost of progressing legislative change and the uncertainty around the continued existence of this mechanism contribute to this option not being considered viable.

Option 4(b) – Using Part 10A of the Privacy Act 1993

Description

Part 10A of the Privacy Act sets up a mechanism to allow an "accessing agency", to have access to an individual's "identity information" held by a "holder agency" for specified purposes.

Analysis

While Part 10A could potentially be used by Police on a case-by-case basis to access identity information held by DIA, this mechanism does not provide for the proactive bulk sharing of name change, death and non-disclosure information. Similar issues as those under options 1 and 2 arise. Option 4(b) partially meets the effectiveness criteria (a). It does not meet the efficiency criteria (b). The privacy criteria (c) and the administrative efficiency criteria (d) could be met. Option 4(b) is not considered a viable option.

Option 4(c) – Bespoke legislative change

Description

Option 4(c) would involve legislative change to the Policing Act 2008 and/or the BDMRRA to create a bespoke system to provide for the sharing of bulk name change, death, and non-disclosure information.

Analysis

While the effectiveness criteria (a), the efficiency criteria (b) and the privacy criteria (c) could all be met, similar to option 4(a) this option runs counter to the intent of setting up the AISA framework in the Privacy Act in the first place (which does not need change to primary legislation). It would likely end up duplicating much of the process steps in the AISA framework just for this specific information sharing between these two specific parties. It therefore does not meet the administrative efficiency criterion (d). Bespoke legislative change is not supported.

In summary

The following table summarises the options analysis. Option 3 meets all the criteria.

	Option 1: status quo	Option 2: MOU	Option 3: AISA	Option 4(a): IMA	Option 4(b): Part 10A Privacy Act	Option 4(c): bespoke legislative change
(a) Effectiveness – improve accuracy	+	+	++	++	+	++
(b) Efficiency – ongoing accuracy	-	-	++	++	-	++
(c) Privacy – appropriate protection	++	++	++	++	++	++
(d) Administrative efficiency	++	++	++	-	++	-
TOTAL	5 + 1 -	5 + 1 -	8 +	6 + 1 -	5 + 1 -	6 + 1 -

Key: ++ meets criteria
+ partially meets criteria
- does not meet criteria

3.2 Which of these options is the proposed approach?

Preferred option – Option 3 - Police and the Registrar-General agree to an Approved Information Sharing Agreement (AISA)

Option 3 is the preferred option.

Description

An AISA would enable the Registrar-General to proactively provide to Police bulk information regarding registered name changes, registered deaths, and non-disclosure directions.

An AISA is a legal mechanism made by Order in Council under Part 9A of the Privacy Act that authorises the sharing of information between agencies to facilitate the provision of public services. Section 78AA of the BDMRRA allows the Registrar-General to disclose birth, death, marriage, civil union, and name change information under an AISA.

AISAs identify the agencies involved in delivering the public services, why they are delivering them, what personal information they need to share, and what they will do with the information, including how they will manage any privacy risks.

Analysis

An AISA can authorise agreed departures from information privacy principles (IPPs) in the Privacy Act if there is a clear public policy justification and the privacy risks of doing so are managed appropriately. In this case, two key IPPs are engaged:

- Under IPP 2, personal information should usually be collected directly from the individual concerned. In this case it is the Registrar-General that collects the information from the individuals concerned (not Police).
- Under IPP 11, personal information should generally only be disclosed where it directly relates to the purpose for which it was obtained. The AISA proposes to enable the Registrar-General to disclose to Police information relating to registered deaths, name changes, and non-disclosure directions. The information was originally collected for purposes relating to the Registrar-General's functions under the BDMRRA, but under the proposed AISA Police would use the information to maintain the law and provide public services.

By providing certainty around information to be shared, an AISA removes doubt around privacy implications and impediments to information sharing under the Privacy Act. AISAs are also public documents.

An AISA can only be made if it meets a certain standard, including having checks and balances in place to protect the privacy of individuals. The Privacy Act prescribes a transparent process to make an AISA, which includes:

- Consulting with the Privacy Commissioner, who can review an AISA once it comes into effect and make other recommendations for change
- Undertaking consultation with affected persons
- Requiring an Order in Council to bring the AISA into force.

Under this option, information would be provided by the Registrar-General to Police in regular bulk batches through a secure file transfer. On receiving the information, Police would run a match against existing records in NIA. If a successful match in NIA is found, the person's NIA record would be updated to show if they are now deceased, have changed their

name, or have a non-disclosure direction in force.

Police will only update existing records in NIA, will not create new records and will not store any identity information on a person that is not already in Police's system. The possible exception will be the creation of a new record in NIA for a person with a non-disclosure direction who has not come into contact with Police before, so that Police will know to protect the name of that individual if they come into contact with them in the future.

Information used to verify an existing identity record and any non-matched data would not be uploaded to NIA or any other Police systems, and will be securely destroyed following completion of the matching process.

This option meets all four criteria. An AISA will help improve the accuracy of information, and do so in an efficient, effective, and timely way. It will also ensure appropriate privacy safeguards are put in place by the parties to protect individual privacy and ensure that any potential interference with privacy is minimised. Police and the Registrar-General consider that it is the only feasible option to meet the criteria, without having to make unnecessary changes to primary legislation.

Section 4: Impact Analysis (Proposed approach)

4.1 Summary table of costs and benefits

Affected parties *(identify)*	**Comment**: nature of cost or benefit (eg ongoing, one-off), evidence and assumption (eg compliance rates), risks	**Impact** *$m present value, for monetised impacts; high, medium or low for non-monetised impacts*
Additional costs of proposed approach, compared to taking no action		
Regulated parties	There are no expected additional costs to individuals whose information is being shared by the Registrar-General. This information is already being collected under the BDMRRA. It is simply being passed on to Police.	Nil
Regulators	There is a one-off administrative cost to government to develop the AISA (primarily on Police and DIA). There is a one-off administrative cost to government to develop the IT system to share the information. This is a relatively small cost within the wider Progressive Steps Project budget ($4.75m), funded from the Justice Sector Fund. There will be ongoing costs to maintain the new IT solution to share the information.	Low, met within Police and DIA baselines Approx $50,000 across DIA and Police Low, met within Police and DIA baselines
Wider government	Not applicable	Not applicable

Other parties	Not applicable	Not applicable
Total Monetised Cost		Approx. $50,000
Non-monetised costs		Low

Expected benefits of proposed approach, compared to taking no action		
Regulated parties	Some individuals and the wider public will receive direct benefits from Police having more accurate information (even if it is just avoiding the undesirable scenarios noted above in section 2.1).	Low
Regulators	More accurate identity information regarding name changes, deaths, and non-disclosure directions will mean Police can provide public services more effectively and efficiently.	Medium
Wider government	There may be some efficiencies passed on to other government agencies in the criminal justice system as a result of Police having more accurate information (eg, Courts, Corrections, etc).	Low
Other parties	Not applicable	Not applicable
Total Monetised Benefit	Not applicable	Not applicable
Non-monetised benefits		Medium

4.2 What other impacts is this approach likely to have?

The proposed AISA will benefit New Zealanders by enabling Police to carry out its law enforcement functions with more accurate information. This is expected to reduce the risks from offenders using multiple identities as well as the number of events relating to misidentified individuals.

There are also benefits to the wider public of enabling Police to have more accurate information about members of the public they engage with, whether as victims, witnesses to a crime, or people that Police is providing or connecting to a service.

Section 5: Stakeholder views

5.1 What do stakeholders think about the problem and the proposed solution?

Public consultation

A public consultation on the proposed AISA was undertaken between 9 October and 6 November 2018. Consultation documentation was published on the Police's website.[1] DIA also posted information about the consultation process on its website. Police contacted some key stakeholders direct to advise them of the consultation. The Minister of Police also issued a media release about the consultation.[2]

Five submissions were received. Of those, two were from individual citizens and three were from organisations (Victim Support, the New Zealand Law Society, and the New Zealand Human Rights Commission). In summary, there was broad support for the AISA across submitters, although three submitters made suggestions to improve/revise the AISA. None opposed the proposed AISA.

Issues raised included the level of specificity with which the draft AISA describes the information to be shared; how the information would be shared; and the policy justification for the AISA covering 'non-offenders' (eg, victims). The majority of submitter feedback, however, covered privacy issues – including:

- comment on the AISA's proposal that Police dispense with the adverse action notice requirement under section 96Q of the Privacy Act
- potential clarification of the wording in clause 9 (Privacy safeguards) of the AISA
- the timeframe for destruction of non-matched information
- communicating with the public that the information will be shared with Police
- potential risk of name change information being released before a non-disclosure direction has been obtained if a person applies for both at the same time
- the process for privacy breaches.

As a result of feedback some changes were made to the draft AISA. These included:

- clarifying the intent/wording of some clauses
- adding in text on the rationale for the AISA applying to all people in NIA (and not just offenders)
- clarifying that information received from the Registrar-General will be destroyed as soon as reasonably practicable
- revising the privacy breach clause around when the Privacy Commissioner will be notified of privacy breaches.

Some issues raised during consultation can be addressed with the development of Operational Procedures to support the AISA (eg, further detail around destruction of information) or via other mechanisms. For example, DIA will revise the privacy notices on its website and information contained in relevant application form instructions to advise people that the information will be shared with Police under the AISA. This will include advising people who apply for a name change and a non-disclosure direction simultaneously that once the name change is registered it will be shared with Police and this may be prior to the non-disclosure direction being approved.

[1] Available at: http://www.police.govt.nz/about-us/programmes-and-initiatives/name-changes-deaths-and-non-disclosure-directions-information

[2] Available at: https://www.beehive.govt.nz/release/information-sharing-help-prevent-crime

The submissions analysis will be published on the Police website with the other AISA documentation once Cabinet has decided whether to approve the AISA.

Consultation with the Privacy Commissioner

The Privacy Commissioner was consulted during the development of the AISA. As a result of this consultation, the draft AISA and associated documents were amended to better explain the policy rationale and to better align the proposed AISA and the Privacy Act's requirements. The Privacy Commissioner provided the following comment:

"The Privacy Commissioner has been consulted throughout the development of this Agreement and appreciates the constructive engagement from officials. He is pleased that Police will not amend their records unless they are certain of an identity match and that sensitive identity information relating to adoption and gender reassignment is excluded from the Agreement. The Commissioner also notes that the Agreement includes specific provisions to protect individuals who have concerns about their safety and who have blocked public access to their DIA records."

Agency consultation

The draft AISA has been consulted with the Ministry of Justice, Department of Corrections, Department of Internal Affairs, New Zealand Customs Service, Ministry of Business, Innovation and Employment (Immigration New Zealand), New Zealand Transport Agency, Ministry of Transport, Te Puni Kokiri, Ministry for Women, Ministry for Pacific Peoples, Ministry of Social Development, Inland Revenue Department, Oranga Tamariki—Ministry for Children, Statistics New Zealand, the Treasury, and Department of Prime Minister and Cabinet (Policy Advisory Group).

Agencies are supportive of the AISA.

Section 6: Implementation and operation

6.1 How will the new arrangements be given effect?

An AISA is approved by an Order in Council made under Part 9A of the Privacy Act. Subject to Cabinet approval, the Order in Council will be drafted by Parliamentary Counsel Office (PCO).

A communications strategy will be developed to support the implementation of the AISA – including a media release, website messaging, and other actions.

The AISA, and supporting documents (including the Privacy Impact Assessment), will be made publicly available on Police's and DIA's websites to give New Zealanders visibility over how and when their personal information will be used. The Order in Council will also be published on PCO's legislation website (www.legislation.govt.nz).

DIA will revise the privacy notices on its website and information contained in relevant application form instructions to advise people that certain information will be shared with Police under the AISA.

Both Police and DIA will develop and agree Operational Procedures to support the implementation of the AISA. These will be consulted on with the Office of the Privacy Commissioner.

The IT system being built to share the information will be tested before 'going live'. This will be maintained by DIA and Police.

If approved, it is expected that the AISA will come into effect by August 2019.

Once in force, DIA will provide a one-off bulk transfer, through a secure file transfer, of all non-disclosure directions on DIA's systems (currently around 95). Regular transfers to Police will capture those registered name changes, death registrations, and non-disclosure directions obtained after the previous transfer of information.

Police will use this information to match against identities in NIA. Matched identities will result in Police amending the NIA record with a new name and any registered names not held in NIA, marking the person as deceased, and/or entering an indicator that a non-disclosure direction is in force. Information used to verify an existing identity record and any non-matched data will not be uploaded to NIA or any other Police systems, and will be securely destroyed following completion of the matching process. Police will only update existing identities in its system and will not store any identity information on persons that is not already in Police's system. The exception will be the creation of a new record in NIA for a person with a non-disclosure direction who has not come into contact with Police before, so that Police will know to protect the name of that individual if they come into contact with them in the future.

Section 7: Monitoring, evaluation and review

7.1 How will the impact of the new arrangements be monitored?

The system, or initially a manual process, will be able to track how many successful matches are made with existing records in NIA (and updates made to NIA). Information on registered deaths will also be used to update the firearms register, although this will be managed manually, not through the system.

Police will take a conservative approach and will not update NIA unless 100% sure of a match. This will require consistency between the data sets, with any unexplained inconsistency precluding a match.

Police and DIA will undertake regular first line assurance and internal audits of the operation of the AISA to confirm that the safeguards in the AISA are operating as intended and remain sufficient to protect the privacy of individuals. This will enable the agencies to check whether any issues have arisen in practice that need to be resolved.

7.2 When and how will the new arrangements be reviewed?

Police will undertake a review six months after the date on which the AISA comes into force by Order in Council. The review will specifically seek to identify the number of successful matches to ascertain whether more (or less) personal information is necessary to achieve full accuracy. A report of this review will be provided to the Privacy Commissioner upon completion.

Following this initial review, further reviews will occur at intervals specified by the Privacy Commissioner. Review reports will be included in Police's annual report.

AISAs are subject to regular review by the Privacy Commissioner. The Privacy Commissioner can review the operation of the agreement on their own initiative 12 months after the Order in Council approving the agreement has been made and at any time that the Commissioner considers appropriate for subsequent reviews.