

# Impact Summary: extending the Targeting Serious Crime information sharing agreement

## Section 1: General information

### Purpose

*Inland Revenue* is solely responsible for the analysis and advice set out in this Regulatory Impact Statement, except as otherwise explicitly indicated. This analysis and advice has been produced for informing final decisions to proceed with changes to be taken by Cabinet.

### Key Limitations or Constraints on Analysis

#### ***Volume of data shared***

It's currently not possible to know how much data will be shared with the two agencies being included in this agreement extension (that is the Serious Fraud Office and Customs). Although initially the number of requests from the Serious Fraud Office is expected to be low (estimated to be less than 20 requests per year), the potential number of requests from NZ Customs will likely be considerably higher (estimated to be more than 200 requests per year).

The low volume of requests has not influenced the preferred choice. However, in the long term, the flexibility provided by the AISA would provide a more sustainable framework for sharing information for serious crime.

### Responsible Manager (signature and date):



Martin Neylan

Senior Policy Advisor

Policy and Strategy – Inland Revenue

20 August 2019

## Section 2: Problem definition and objectives

### 2.1 What is the policy problem or opportunity?

Section 18 of the Tax Administration Act 1994 provides a strict rule of taxpayer confidentiality, meaning Inland Revenue (IR) is not allowed to share a taxpayer's information with other agencies. Inland Revenue is not authorised to proactively send individual information to other agencies and is also very restricted in its ability to respond to information requests. Responding to requests from other agencies is only permitted where there is an express statutory exception to confidentiality, and these exceptions are very limited.

In 2014, IR became party to an approved information sharing agreement (AISA) with the New Zealand Police (Police) to help reduce the level of serious crime<sup>1</sup> committed in New Zealand. The original intent behind the implementation of the agreement was to provide an all-of-Government response to law enforcement, which identified, among other things, the need for improved information sharing.

At the time the agreement between IR and the Police was introduced, numerous other government departments in the enforcement area expressed interest in information held by IR to enable them to work more effectively, but for various reasons did not take part in the agreement. More recently, the NZ Customs Service (Customs) and the Serious Fraud Office (SFO) demonstrated interest in receiving information from IR for tackling serious crime.

The agreement between IR and the Police has proved successful, facilitating the investigation of over 500 cases, and an average cost below \$14,000 per year in the last three years of operation. Officials have been looking at ways to facilitate the sharing of IR information with SFO and Customs to further help tackle serious crime. Sharing information with these agencies would enable better use of their resources and achieve improved results in the area of law enforcement.

The proposed initiative is to facilitate the sharing of information between IR and the SFO and Customs to assist identification, investigation and prosecution of serious crimes involving fraud and corruption or cross-border crime.

### 2.2 Who is affected and how?

Increased sharing of tax information carries potential societal benefits in the area of law enforcement. The primary benefit of making IR information more available in the law enforcement area is that the Government is better able to enforce its laws in relation to serious crime, including serious financial crime. This improves New Zealand's reputation as a safe place, for New Zealanders as well as overseas parties, to deal or transact in and as a country with effective Government institutions.

The group affected by this sharing of information would be people engaged in serious

<sup>1</sup>Serious crime is defined in the Serious Crime AISA as an offence punishable by a term of imprisonment of four years or more.

criminal activity. Implementing information sharing between agencies for targeting serious crime may drive change of behaviour of people in this group, making them less inclined to be involved in serious crime not only within New Zealand, but also overseas, of people who may currently perceive New Zealand as an easy environment for committing crime (cross-border crime usually involves an overseas and a New Zealand party, and since information will be shared with Customs, it would be easier to track associations). At the same time, it is not expected that sharing information for serious crime would impact on tax compliance as the public is supportive of information sharing for this purpose.

Public opinion<sup>2</sup> indicates that information should flow freely across Government departments; that serious criminals should not be protected by privacy laws; and that easier sharing of information across the Government would result in more resources being freed up and increase the detection of people committing serious crimes. At an individual level, people would like their information to be kept confidential, but at a community level, people believe absolute confidentiality should not be extended to those engaging in illegal behaviour, provided that good processes are in place to manage any sharing of information.

The initiative is consistent with the Government's commitment to making communities safer and reducing crime. It also supports the Government's objective of giving the New Zealand Police and the New Zealand Customs Service the resources they need to "crack down" on gangs, organised crime and drug trafficking.

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

The analysis has considered different models for the sharing of information, which include the flows of information and the structure of the sharing. The sharing should maintain the current state of the information sharing between the Police and IR, justified by the successful operation of the current agreement. The information sharing for serious crime only builds a stronger case to get support from the public.

Regarding the sharing model structure, a "one-to-many" sharing agreement (meaning one agency, being IR, sharing with all the others), and a "many-to-many" sharing agreement (meaning sharing occurring between all agencies) have been considered. A one-to-many model is the preferred one, given the legal complexities involved in a many-to-many model.

Regarding the flows of information, a one-way (proactive and reactive) sharing agreement will be introduced between IR and SFO/Customs. This is based on the existing sharing agreement with the Police. IR will provide information to SFO/Customs upon request or proactively when IR identifies evidence of a potential serious crime relevant to those agencies. The provision of information from the other agencies to Inland Revenue relies on one of the exceptions to Privacy Principle 11 of the Privacy Act,<sup>3</sup> and therefore has not been included in the original or the proposed information sharing.

<sup>2</sup> Public consultation undertaken in 2014 for the Serious Crime AISA between IR and NZ Police

<sup>3</sup> Privacy Principle 11: Limits on disclosure of personal information – An agency that holds personal information shall not disclose the information to a person or body or agency unless the agency believes, on reasonable grounds, (e) that non-compliance is necessary (i) to avoid prejudice to the maintenance of the law, and (iii) for the protection of the public revenue.

In terms of connections, this initiative supports the latest State Sector Act Reform proposals<sup>4</sup> approved by Cabinet in June this year, where the changes would see the Public Service operate as one, joined up system to tackle the big, complex challenges facing New Zealand.

Earlier this year, there were changes made to the TAA in relation to the confidentiality rules. However, the impact of those changes on this proposed agreement is not a constraint, but rather an enhancement.

One of the changes concerns the reuse of information: “information gathered for one purpose being used for other purposes within Inland Revenue”. That change in particular can potentially affect the proposed information sharing agreement positively, making it more flexible and efficient.

---

<sup>4</sup> <http://www.ssc.govt.nz/resources/consultation-state-sector-act-reform/>

## Section 3: Options identification

### 3.1 What options have been considered?

In considering the options for this initiative the following criteria have been used to shape the decision-making process:

- Efficiency of administration – gain efficiencies through a more collaborative, cross-agency work, including timeliness of implementation, coverage of agreement (wider inclusion of government agencies), and costs for the Government
- Fairness and integrity – maintain the integrity of the tax and benefit systems, and ensure sufficient protection of people’s privacy and a proper level of security and transparency
- Sustainability of the public sector – provide a framework that is flexible enough to respond to Government’s priorities, and facilitate changes going forward.

As the problem is a lack of legislative authority to share information between the agencies, there are no non-regulatory options to enable information sharing to occur. The following options have been considered to enable the information sharing:

#### **Option One:** Status quo

*Efficiency of administration:* IR is bound by the confidentiality rules in the Tax Administration Act 1994, so the information sharing cannot occur.

*Fairness and integrity:* this option protects people’s privacy by not sharing taxpayer information IR holds. On the other hand, for serious crime, being able to share information held by multiple government agencies can help with building a picture more precisely and more efficiently. If agencies do not have the flexibility to do so, it may limit or hinder an investigation of serious crime.

*Sustainability of the public sector:* This is not a sustainable option because it does not enable agencies to work together and is not effective at achieving the policy objective.

#### **Option Two:** Sharing information under an AISA under the Privacy Act, which is allowed for under section 18E(2) of the Tax Administration Act 1994 (**preferred option**)

*Efficiency of administration:* This option enables cross-agency collaboration and provides a framework that allows subsequent amendments to be made in an efficient manner.

*Fairness and integrity:* The AISA clarifies and improves the rules around how agencies share personal information, while ensuring safeguards are in place to protect an individual’s privacy. It would provide certainty around the purpose of information sharing, use of information, and management of privacy risks; it can also modify privacy principles when justified. AISAs provide a transparent approach to sharing, as all agreements are made public and consultation is required for any agreement.

*Sustainability of the public sector:* An AISA is easier and faster to amend to include sharing of additional information and also including other agencies in comparison to the process for



changing legislation, providing a more future-proof framework for sharing information.

**Option Three:** Legislating specific exceptions to the tax confidentiality rules to enable information sharing between the agencies to occur.

*Efficiency of administration:* This option is time consuming to enact and any subsequent amendment to that legislation would also be time consuming. It's also limited by the fact that it is very specific.

*Fairness and integrity:* This option has the advantage of being the most transparent. The information sharing would face Parliamentary scrutiny and would be recorded in primary legislation.

*Sustainability of the public sector:* while this option enables sharing of information between agencies, it is a rigid model and doesn't provide a framework on which other agencies can build on. This is not a sustainable option because it does not provide the required flexibility going forward.

**Option Four:** Sharing information under section 18F of the Tax Administration Act which requires an Order in Council

*Efficiency of administration:* This option takes about the same time to implement as option 2 (AISA). However, an AISA is considered the most appropriate mechanism to share personal information, even when the share involves some non-personal information.

*Fairness and integrity:* This option ensures sufficient protection of people's privacy and a proper level of security and transparency. It requires consultation with the Privacy Commissioner and affected organisations before an Order in Council is made to enable the information sharing.

*Sustainability of the public sector:* Section 18F is a mechanism more appropriate for sharing non-personal information. This is not the case for serious crime, which involves personal information.

### 3.2 Which of these options is the proposed approach?

For the reasons outlined in section 3.1 above, the most appropriate mechanism for sharing information in this case, and therefore the proposed approach, is an AISA (option two). Since there is an AISA for tackling serious crime between IR and the Police, a decision has been made to extend the agreement to include information sharing with the SFO and Customs, rather than creating a new agreement for the same purpose.

The new (extended) agreement will retain the same framework used to share information with the Police, which means the same purpose of sharing and the rules around it will be maintained.

The proposed approach is not incompatible with the Government's 'Expectations for the design of regulatory systems'.

## Section 4: Impact Analysis (Proposed approach)

### 4.1 Summary table of costs and benefits

Affected parties ( <i>identify</i> )	<b>Comment:</b> nature of cost or benefit (eg ongoing, one-off), evidence and assumption (eg compliance rates), risks	<b>Impact</b> \$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 ( <i>people engaging in serious crimes involving fraud, corruption or cross-border activities</i> )	There will likely be additional costs to people who are engaged in serious criminal activity. If they are investigated they may need to incur the costs for professional services (e.g. lawyers, accountants). The likelihood of them being investigated as a result of information being shared between agencies will increase, as it will become easier to detect connections and build cases.  However, if they become compliant, which is one of the expected benefits of implementing information sharing for tackling serious crime, there will be no costs to them.	Medium/High (when the parties are engaged in serious criminal activity)
Regulators ( <i>IR, SFO and Customs</i> )	Implementation costs would be minimal, and funding will be undertaken within departmental baselines.	Low
Wider government	None identified.	Nil
Other parties	None identified.	Nil
<b>Total Monetised Cost</b>		Low
<b>Non-monetised costs</b>		Low

#### Expected benefits of proposed approach, compared to taking no action

Regulated parties ( <i>people engaging in serious crimes involving fraud, corruption or cross-border activities</i> )	There are no benefits for this group, because these would be people engaged in serious criminal activities and not supposed to get benefits from the information sharing agreement.  Instead, as the information share should support investigation and prosecution of serious criminal activity, it should act as a deterrent for the group to engage in further criminal activity.	Nil
--	--	-----



Regulators (IR, SFO and Customs)	Ability to build stronger cases when identifying serious crime, due to a more complete picture provided by the information shared. An information sharing agreement with the relevant agencies will create efficiencies through more collaborative, cross-agency work. The agreement will improve the agencies' ability to enforce Serious Crime under the Crimes Act 1961, the Customs and Excise Act 2018, and the Serious Fraud Office Act 1990, and hold non-compliant businesses and individuals responsible for unlawful activities to account.	High  <i>Note:</i> the information sharing with the Police has facilitated over 500 investigations in the last three years. It is estimated that the extension of the agreement to Customs and SFO will add over 200 investigations per year to the current number of investigations.
Wider government	None identified.	
Other parties	There are benefits for wider society, from a potential decrease in serious criminal activity, due to the Government's ability to have it more efficiently controlled.	Medium/High
<b>Total Monetised Benefit</b>		Unable to estimate
<b>Non-monetised benefits</b>		<i>High</i>

## 4.2 What other impacts is this approach likely to have?

In the case of organised criminal activity, the benefits to society of sharing information outweigh the reduction in privacy of certain individuals and the risks to the voluntary compliance model on which our tax system is based. This has been confirmed by research undertaken about information sharing and its impact on compliance, which reports that people's trust in government and compliance would not be affected, as long as the purpose for the information sharing is clearly defined.<sup>5</sup>

Serious crime has a number of components that may be taken into account when considering the big picture. Being able to share information held by multiple government agencies can help with building that picture more precisely and more efficiently. This, in turn, will prevent harm to other businesses and individuals, and promote public confidence in the integrity of New Zealand's personal and business environment, benefiting the New Zealand economy as a whole.

## Section 5: Stakeholder views

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

The following agencies have been consulted and either support or do not object to the proposed agreement:

- the New Zealand Police
- the Ministry of Justice
- the Treasury
- the Department of the Prime Minister and Cabinet, and
- the Office of the Privacy Commissioner.

The Office of the Privacy Commissioner was consulted during the initial AISA drafting process and will continue to participate in active consultation with IR, the SFO and Customs as the AISA progresses through public consultation and as operational processes are developed.

Two submissions were received from public consultation, both from organisations – the Chartered Accountants Australia and New Zealand (CAANZ), and the New Zealand Law Society (NZLS). Submitters raised very similar concerns to the ones raised in previous consultation on the Serious Crime AISA. The points raised, and the officials' responses are as follows:

*Inland Revenue's officers do not have the appropriate experience or expertise to correctly identify possible criminal offences outside their area of action (e.g. smuggling or drug*

<sup>5</sup>ThinkPlace, *Information Sharing and Tax Compliance, How might people change their behaviour?*, July 2018

*offences*). – A small dedicated team comprised of experienced investigators with specialised training would be managing the information sharing with the other agencies. In addition to undergoing a ‘test for sharing’, information would only be shared proactively when identified during the team’s normal course of activities.

*Using taxpayer information for non-tax purposes unjustifiably limits taxpayers’ fundamental rights and undermines the integrity of the tax system. The AISA extension unduly infringes taxpayer’s right to be free from unreasonable search and seizure, and the privileges against self-incrimination.* – The AISA extension does not change the exercise of the Commissioner of Inland Revenue’s statutory powers or curtails taxpayers’ fundamental rights. Officials believe that the benefits of sharing information for reducing societal harm from criminal activity outweigh the reduction in privacy in those specific cases. The AISA is consistent with the Information Privacy Principles’ exceptions in the Privacy Act which already exist alongside the privilege against self-incrimination in the Evidence Act. In addition, the proposal simply extends to Inland Revenue an exception that already applies to most Government agencies, and at the same time provides parameters to control and limit the information sharing.

*Innocent third parties may be affected by the information sharing and their interests should be protected.* – For every request for information, the relevance of obtaining information about linked parties needs to be justified. There is a strict test to be applied before any information can be shared (proactively or on request).

*A victim’s consent should be sought before their personal information is shared.* – The ‘test for sharing’ is applied to ensure the information has relevance to the investigation and the intent of the sharing. In some cases, informing and obtaining consent from the victim may prejudice the investigation and have an adverse effect. In cases of serious crime covered by Customs (e.g. money laundering, drug trafficking) generally there isn’t a victim as an individual. In the case of the Serious Fraud Office, the crimes being committed may have multiple victims (e.g. fraud committed against a large group of people) and may be impractical to obtain consent from all the victims.

*People should be informed when providing information to Inland Revenue under compulsion that the information may be provided to other agencies.* – Inland Revenue advises taxpayers either at the point of collection (e.g. forms) or through information published on its website that their information may be shared with other agencies, and that collection is authorised by law. When the information is collected under coercive powers (e.g. sections 17 and 17B of the TAA), Inland Revenue is required to consider the provenance of information and whether any particular security arrangements are needed, rather than having a blanket restriction on sharing that information.

Information obtained under compulsion under sections 17I and 17J of the TAA is not currently shared and is of limited use to other agencies given that the sections restrict how this information may be used in court. The agreement extension does not propose to change that, and clarifies that information obtained under these sections would not be shared, unless the other agency has the same power to obtain that information.

Further, the AISA includes a provision to dispense with giving notice of adverse action to the individual affected (in accordance with section 96R of the Privacy Act) because giving notice would “tip off” an alleged serious criminal offender.

*There is a low threshold for information sharing under the AISA and many offences that fall short of truly serious offending are captured.* – The four-year threshold aligns with the test for the offence of participation in an organised criminal group (section 98A of the Crimes Act) and is consistent with the definition of a ‘serious crime’ contained in the United Nations Convention against Transnational Organised Crime.

## Section 6: Implementation and operation

### 6.1 How will the new arrangements be given effect?

It is planned that the AISA will be enacted in the first half of 2020, after an Order in Council is made. IR is the lead agency for the agreement and responsible for introducing the 'Request for Information' requirements to the other agencies. This work has been already assessed and requires minor changes to the current process that is used to share information with the Police.

#### ***System or Technology Impacts***

For IR, implementation impacts would be minimal. The current process would be replicated for the other additional agencies, and the same operational units would continue to handle the requests for information utilising existing resources. The proposed changes do not include any systems or technology changes as the information shared is compiled manually on a case-by-case basis and sent by secure email (SeeMail).

For the SFO, there would be no or little implementation impact. The SFO is already equipped to receive, store and review information from IR as appropriate, and would use existing channels to continue to do so.

Customs would use existing information technology systems and processes to manage information shared by IR, with appropriate mechanisms to ensure confidentiality of taxpayer information.

#### ***Implementation costs***

For all three agencies, implementation costs would be minimal, and funding will be undertaken within departmental baselines.

## Section 7: Monitoring, evaluation and review

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

IR is required to report to the Privacy Commissioner each year on the operation of the AISA. The report is concerned with whether the agreement is meeting its goals and may cover:

- the costs and benefits of sharing
- difficulties experienced
- audits undertaken
- amendments and safeguards put in place
- complaints received
- number of individuals whose information has been shared
- number of transactions that have occurred, and
- number of adverse actions taken as a result.

Reports are administered and stored by the Information Sharing Team at IR.

### 7.2 When and how will the new arrangements be reviewed?

AISAs are subject to review by the Privacy Commissioner. The Privacy Commissioner can review the operation of the agreement on his or her 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.

Any review by the Privacy Commissioner would cover whether the agreement is failing to meet its goal in facilitating public services, unreasonably infringing privacy, or operating in an unforeseen way. It would also cover whether the costs of sharing are outweighing the benefits. If there are reasonable grounds to believe any of these are occurring, the Privacy Commissioner will prepare a report for the Minister of Revenue, which will also be tabled in Parliament, recommending changes or termination of the agreement.