

Hon Stuart Nash, Minister of Revenue

Hon Jenny Salesa, Minister of Customs

Information Release

Extending the serious crime information sharing agreement

December 2019

Availability

This information release is available on Inland Revenue's Tax Policy website at <http://taxpolicy.ird.govt.nz/publications/2019-ir-cab-swc-19-sub-0128/overview>.

Documents in this information release

1. IR2019/009 RPT19/030 – Tax policy report: Consultation on extending the serious crime information sharing agreement – report on submissions (22 August 2019)
2. SWC-19-SUB-0128 – Cabinet paper: Extending the serious crime information sharing agreement consultation – summary of submissions (18 September 2019)
3. SWC-19-SUB-0128 – Information sharing agreement between Inland Revenue and New Zealand Police, New Zealand Customs Service and Serious Fraud Office (August 2019)
4. SWC-19-SUB-0128 – Letter from the Privacy Commissioner: Privacy Commissioner's submission on the proposed extension to the information sharing agreement with the New Zealand Police to prevent, detect, investigate or provide evidence of serious crime (20 August 2019)
5. SWC-19-SUB-0128 – Regulatory impact assessment: Extending the targeting serious crime information sharing agreement (20 August 2019)
6. SWC-19-MIN-0128 – Minute: Extending the serious crime information sharing agreement (18 September 2019)

Additional information

The Cabinet paper was considered by the Cabinet Social Wellbeing Committee on 18 September 2019 and confirmed by Cabinet on 23 September 2019.

One attachment to the tax policy report (IR2019/009 RPT19/030) is not included in this information release as it is publicly available:

- The New Zealand Law Society's submission on the *Targeting serious crime: extending information sharing* discussion document (2 November 2018).

Information withheld

Some parts of this information release would not be appropriate to release and, if requested, would be withheld under the Official Information Act 1982 (the Act). Where this is the case, the relevant sections of the Act that would apply are identified. Where information is withheld, no public interest was identified that would outweigh the reasons for withholding it.

Sections of the Act under which information was withheld:

9(2)(a) to protect the privacy of natural persons, including deceased people

Copyright and licensing

Cabinet material and advice to Ministers from the Inland Revenue Department and other agencies are © Crown copyright but are licensed for re-use under the Creative Commons Attribution 4.0 International (CC BY 4.0) licence (<https://creativecommons.org/licenses/by/4.0/>).



For material created by other parties (such as submissions), copyright is held by them and they must be consulted on the licensing terms that they apply to their material.



POLICY AND STRATEGY

Tax policy report: Consultation on extending the Serious Crime information sharing agreement – report on submissions

Date:	22 August 2019	Priority:	Medium
Security level:	In Confidence	Report number:	IR2019/009
		Report no. Customs:	RPT19/030

Action sought

	Action sought	Deadline
Minister of Revenue Minister Responsible for the Serious Fraud Office	Sign the attached Cabinet Paper and forward it to the Cabinet Social Wellbeing Committee Office	10am, 12 September 2019
Minister of Customs	Sign the attached Cabinet Paper and return it to the Minister of Revenue	11 September 2019

Contact for telephone discussion (if required)

Name	Position	Telephone
Martin Neylan	Senior Policy Advisor Inland Revenue	s 9(2)(a)
s 9(2)(a)	Policy Analyst Inland Revenue	
	Policy Analyst New Zealand Customs Service	
Paul O'Neil	General Counsel Serious Fraud Office	

22 August 2019

Minister of Revenue
Minister Responsible for the Serious Fraud Office
Minister of Customs

Consultation on extending the Serious Crime information sharing agreement – report on submissions

Executive summary

1. This report provides an overview and high-level analysis of submissions received on the discussion document *Targeting Serious Crime¹: Extending information sharing*, and the associated draft approved information-sharing agreement (AISA), which were released for public consultation at the end of September 2018. The discussion document proposed extending the existing Serious Crime AISA between Inland Revenue and the New Zealand Police (Police) to include two additional agencies: the Serious Fraud Office, and the New Zealand Customs Service (Customs).

2. The Serious Crime AISA was implemented in 2014. Extending the information sharing to the Serious Fraud Office and Customs under the same agreement would enable Inland Revenue to share information with those agencies, to enable them to carry out more thorough investigations, and to detect a broader range of serious offences.

3. Two submissions were received during the consultation period: one from Chartered Accountants Australia and New Zealand (CAANZ), and one from the New Zealand Law Society (the Law Society). Most concerns raised in the submissions are similar to those raised in the 2013 consultation on the original information-sharing agreement between Inland Revenue and the Police.

4. Submissions raised the following points:

- concerns that the increasing information-sharing activity by Inland Revenue may undermine the integrity of the tax system
- concerns that the AISA unduly infringes taxpayers' right to be free from unreasonable search and seizure, and the privilege against self-incrimination
- concerns that the serious crime definition threshold was set at too low a level and would result in the sharing of information concerning offences that fall short of truly serious offending
- the need to protect the interests of innocent third parties who may be affected by the information sharing
- the need to ensure transparency and include notification processes (victims' consent and information obtained under compulsion), and

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

- concerns regarding the expertise of the Inland Revenue team managing the proactive disclosures.

5. The concerns have been considered by officials and, where possible, have been addressed. The draft AISA has been amended accordingly.

6. In deciding whether to proceed with the AISA, the Privacy Act requires the Minister of Revenue to have regard to the submissions received and be satisfied that:

- the sharing will facilitate the provision of any public services;
- the personal information to be shared is necessary to facilitate the provision of that public service;
- the agreement does not unreasonably impinge on the privacy of individuals;
- the benefits of sharing personal information are likely to outweigh the costs of sharing it; and
- any potential legislative conflicts have been appropriately addressed.

7. The Privacy Commissioner has reviewed the AISA and considers that the AISA meets the above requirements of the Privacy Act.

8. This report recommends that you agree to proceed with the extension of the Serious Crime AISA pursuant to the Privacy Act 1993 (Privacy Act), which provides for the sharing of information between Inland Revenue and the Serious Fraud Office, and between Inland Revenue and Customs.

9. This report also recommends that you approve the repeal of the current information-sharing provision between Inland Revenue and the Serious Fraud Office to address legislative conflicts with the AISA. The repeal will take effect from a future date set by Order in Council. This is to ensure that there is only one authorising provision in force at any point in time to enable information sharing between the two agencies.

10. If you agree with the recommendations to progress this proposal, officials recommend Ministers sign the attached Cabinet paper for referral to the Social Welfare Committee for their approval.

Recommended action

11. We recommend that Ministers:

- (a) **Note** the comments from submitters and officials' responses in this report, and the attached submissions.

Noted

Noted

- (b) **Note** that, in deciding whether to recommend the making of an Order in Council, the Minister of Revenue must consider and be satisfied that:

- i. the information-sharing agreement will facilitate the provision of any public service or public services
- ii. the type and quantity of personal information to be shared under the agreement are no more than is necessary to facilitate the provision of that public service or those public services
- iii. the agreement does not unreasonably impinge on the privacy of individuals, and contains adequate safeguards to protect their privacy

- iv. the benefits of sharing personal information under the agreement are likely to outweigh the financial and other costs of sharing it, and
- v. any potential conflicts or inconsistencies between the sharing of personal information under the agreement and any other enactment have been identified and appropriately addressed.

Noted

Noted

- (c) **Note** that the Privacy Commissioner has reviewed the draft AISA, and confirms that the AISA meets the requirements of an AISA as set out in the Privacy Act 1993, as outlined in recommendation (b) above.

Noted

Noted

- (d) **Agree** with the repeal of the current legislative information-sharing provision between Inland Revenue and the Serious Fraud Office (Schedule 7 clause 7 of the Tax Administration Act 1994) to address legislative conflict with the AISA.

Agreed/Not agreed

Agreed/Not agreed

- (e) **Agree** to proceed with the extension of the Serious Crime AISA pursuant to the Privacy Act, which provides for the sharing of information from Inland Revenue to the Serious Fraud Office, and to the New Zealand Customs Service.

Agreed/Not agreed

Agreed/Not agreed

- (f) If Ministers agree to proceed with the AISA, **sign and refer** the attached Cabinet paper to the Cabinet Office for consideration by the Cabinet Social Wellbeing Committee.

Signed and referred

Signed

12. We recommend that the Minister of Revenue:

- (g) **Refers** a copy of the attached Cabinet paper to the Minister of Finance for his information.

Referred

Martin Neylan
Senior Policy Advisor
Policy and Strategy
Inland Revenue

Paul O'Neil
General Counsel
Serious Fraud Office

Anna Cook
Director Policy
Policy, Legal and Governance
New Zealand Customs Service

Hon Stuart Nash
Minister of Revenue
Minister Responsible for the Serious Fraud Office

/ /2019

Hon Jenny Salesa
Minister of Customs

/ /2019

Background

13. The discussion document (*Targeting Serious Crime: Extending information sharing*) released at the end of last year presented the proposals for extending the existing Serious Crime AISA (the information-sharing agreement between Inland Revenue and the Police for tackling serious crime) to include the Serious Fraud Office and Customs.

14. The proposed extension of the Serious Crime AISA would be under the same framework used for the original agreement: information is shared to identify, investigate and prosecute serious crime, and the sharing of information must meet a set of criteria (the 'test for sharing' framework explained below). By expanding the AISA to include the Serious Fraud Office and Customs, Inland Revenue would be able to share information with these agencies to help investigations of fraud, corruption and cross-border offences that fit the serious crime definition.

15. Information provided by Inland Revenue would assist in providing new leads to an investigation and would also strengthen serious criminal cases such as fraud, financial crime, money laundering and drug trafficking.

16. A 'test for sharing' is applied to any information request or proactive sharing under the Serious Crime AISA. A set of conditions must be met before the sharing of information is considered:

- there are reasonable grounds for suspecting that a serious crime has been committed, is being committed, or will be committed
- the agency considers that there are reasonable grounds for suspecting the information is relevant to the prevention, detection, investigation, or providing evidence of a serious crime, and
- the information is readily available within Inland Revenue, and that it is reasonable, practicable and in the public interest to provide the information to the other agency.

17. Submissions from previous consultation indicate that, in general, information should flow freely across government departments to detect and prevent crime. Although the submissions at the time generally favoured the proposals, some concerns were raised. Submitters' concerns were addressed by officials as part of the original AISA consultation process [Policy report PRI 08-04, BR/13/320, PAS2013/241 refers].

Discussion of submissions

Overview

18. Two submissions (appendices A and B) were received during the public consultation period for this AISA extension, both from organisations. Chartered Accountants Australia and New Zealand (CAANZ) support the proposals but provide some recommendations. The New Zealand Law Society (Law Society) has concerns with the agreement extension that are similar to those they raised in the 2013 consultation on the original information-sharing agreement between Inland Revenue and the Police. After the consultation period closed, officials met with Law Society's representatives to discuss their concerns further.

19. The Law Society's primary concern, which it clarified relates not only to this AISA but also to increased information sharing by Inland Revenue generally, is that sharing information that has been collected for purposes that are not strictly tax-related undermines the integrity of the tax system.

20. The Law Society considers that crime-related information should only be shared in the most serious of cases. This reflects the traditional view that voluntary compliance with tax obligations depends on Inland Revenue maintaining secrecy, and that Inland Revenue has strong information-gathering powers on the understanding that information will be kept secret. The Law Society also considers that information obtained by compulsion should not be shared with other agencies that do not have those same powers.

21. The Law Society's concern is that Inland Revenue's obligation to maintain the secrecy of the information it holds has been eroded over time with the introduction of more and more secrecy exceptions, without revisiting whether there should consequently be a reduction in Inland Revenue's information-gathering powers.

22. Inland Revenue acknowledges that many exceptions to secrecy have been introduced into the Tax Administration Act 1994 (TAA) over the years, and this has generally not been associated with a discussion about information gathering powers. Inland Revenue also acknowledges that, whereas exceptions were initially introduced to facilitate the performance of tax-related functions, there are also exceptions that are aimed at achieving wider public policy goals.

23. Inland Revenue holds a unique set of information within government, which can be used to achieve worthwhile outcomes in the public interest. However, unlike other agencies that can share information in accordance with exceptions to privacy principles in the Privacy Act, Inland Revenue is subject to secrecy obligations and cannot do the same, even though many of Inland Revenue's information-sharing initiatives are essentially for purposes that align with those exceptions in the Privacy Act.

24. Each time a secrecy exception has been added, or a new information-sharing arrangement entered into under secondary legislation, consultation has been undertaken, either in the form of public consultation, or through Select Committee scrutiny to help ensure that it is the type of sharing that the public considers is appropriate for a revenue agency to be undertaking. In addition, the Office of the Privacy Commissioner (OPC) has oversight of many of Inland Revenue's information-sharing initiatives, including the Serious Crime AISA extension, and they are comfortable with what is currently proposed.

25. Inland Revenue also undertakes research² on public attitudes to its information sharing from time to time, to ensure that it understands the potential impacts of its information sharing on voluntary compliance, and public perceptions of the integrity of the tax system, so that it can align its information-sharing initiatives with the "social licence" it considers it holds at the time.

26. Feedback that Inland Revenue has received in consultation and via surveys is that the public generally approve of information-sharing that benefits society, either by facilitating the provision of public services or by helping to uphold the law. Feedback does not indicate that there is likely to be a significant impact on voluntary compliance or that Inland Revenue's information-gathering powers should be restricted as a result.

27. Inland Revenue notes that the government has recently agreed to reduce the scope of secrecy itself, as part of the Taxation (Annual Rates for 2018-19, Modernising Tax Administration, and Remedial Matters) Act. The aim of the amendments is to better target the currently very broad secrecy rule to protecting information about taxpayers. The changes are largely designed to enable more transparency about Inland Revenue's operations (where appropriate), and more sharing via regulation or with taxpayer consent.

² ThinkPlace, Information Sharing and Tax Compliance, How might people change their behaviour?, July 2018
Professor Miriam Lips, Dr Elizabeth Eppel, Amanda Cunningham & Virginia Hopkins Burns, Public Attitudes to the Sharing of Personal Information in the Course of Online Public Service Provision, Victoria University of Wellington, 2009.

Inland Revenue, Information sharing between government agencies – Cultural perspectives, Inland Revenue, 2012.

28. In the absence of recent case law that is specifically on point, it is hard to know how the Courts might view the recent amendments to Inland Revenue's secrecy obligations. However, in light of the consultation processes and research referred to above, Inland Revenue considers that it has some justification for having changed its information-sharing approach over time to reflect modern expectations of transparency and efficient government administration.

29. Inland Revenue notes that it invests a great deal of time and resources into ensuring that its information-sharing arrangements are subject to the appropriate controls so that it only shares what is necessary to meet the purpose of the arrangement, and that decisions about what information should be shared are made by those with the appropriate skills. Officials ensure that information is transmitted and stored securely, and privacy protections are in place.

Taxpayers' right to be free from unreasonable search and seizure, and the privilege against self-incrimination

30. The Law Society's view is that the AISA extension unduly infringes taxpayers' right to be free from unreasonable search and seizure, and the privilege against self-incrimination. Representatives of the Law Society believe that the agencies receiving information from Inland Revenue would be taking advantage of Inland Revenue's coercive powers to obtain information that they would not be able to obtain otherwise. They recommended there should be an 'enduring concrete safeguard' against misuse of the AISA in this respect. They also suggested that, when people are providing information to Inland Revenue under compulsion, they should be informed that the information may be provided to other agencies.

31. The right to be free from unreasonable search and seizure, in section 21 of the Bill of Rights Act 1990³ (NZBoRA), protects against unreasonable state intrusion into an individual's privacy. Any information sharing must not breach that section, which prohibits unreasonable searches. To the extent that the AISA extension imposes limits on this right, this constitutes a reasonable limitation in terms of section 5 of the NZBoRA⁴.

32. The privilege against self-incrimination (or 'right to silence') is set out in section 60 of the Evidence Act 2006. Certain powers of the Commissioner of Inland Revenue override this right, meaning that taxpayers cannot refuse to provide documents sought by the Commissioner under sections 17I and 17J⁵ of the TAA, nor can a taxpayer refuse to comply with an inquiry under sections 18 or 19⁶ of the TAA on the basis that their answers may incriminate them.

33. However, information obtained under sections 18 and 19 is unable to be used in criminal proceedings against the person (except for cases of perjury). The bar on use of information obtained pursuant to sections 18 and 19 proceedings is not limited to tax-related proceedings, but rather covers all criminal proceedings. This proposal will not change that bar. The draft AISA has been amended to reflect the limitations on sharing information obtained under sections 18 and 19 of the TAA, and to avoid unreasonable search and seizure.

³ Section 21 - Unreasonable search and seizure - Everyone has the right to be secure against unreasonable search or seizure, whether of the person, property, or correspondence or otherwise.

⁴ Section 5 - Justified limitations – Subject to section 4, the rights and freedoms contained in this Bill of Rights may be subject only to such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society.

⁵

⁶ Section 18 – Inquiry before a District Judge; section 19 – Inquiry by Commissioner

34. The Law Society's preferred approach is that information obtained by compulsion under Inland Revenue's collection powers (sections 16 to 19 of the TAA) should not be shared with other agencies that do not have those same powers.

35. The OPC made a similar point in submitting on the proposed changes to the information sharing provisions in the Taxation (Annual Rates for 2018-19, Modernising Tax Administration, and Remedial Matters) Bill in 2018. In its submission, the OPC recommended including additional safeguards for the on-sharing of information obtained under mandatory collection powers and disclosed under an information-sharing agreement.

36. As a result, a compromise position was achieved whereby Inland Revenue will be required to consider the provenance of information and whether any particular security arrangements are needed, rather than including a blanket prohibition on sharing information obtained by compulsion.

37. Officials consider this is a reasonable approach as a blanket restriction on sharing such information has not been included in the TAA and the Privacy Act does not contain any provisions that would limit the sharing of such information in the context of the Approved Information Sharing Agreement (AISA) regime.

38. In the context of the Serious Crime AISA, the participating agencies have similar compulsion powers. However, other sharing arrangements where partner agencies do not have such powers would need to be considered on a case-by-case basis.

39. It should be noted that any information that Inland Revenue discloses to other agencies under an information-sharing agreement will be from information that Inland Revenue already has readily available. Under no circumstances will Inland Revenue exercise its powers to collect information on behalf of the other agencies, nor share personal information that is not already readily available within Inland Revenue and/or not relevant to the serious crime in question.

40. Inland Revenue advises taxpayers that their information may be shared with other agencies through the relevant forms/guides, or this information is in the privacy policy published in the Inland Revenue website. Inland Revenue considers that it would be inappropriate to notify taxpayers before sharing information with another agency under the proposed AISA, as this would put the person on notice that they were subject to a criminal investigation. This would render the information-sharing ineffective.

The threshold for information sharing under the AISA (definition of serious crime)

41. The Law Society argues that there is a low threshold for information sharing under the AISA, and that many offences fall short of truly serious offending are captured. They suggested that the definition of 'serious crime' should be more specific to each agency, limited to particular crimes rather than a penalty, or that the penalty limit in the definition should be raised.

42. The AISA applies to offending that may result in four years imprisonment. 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' in the United Nations Convention against Transnational Organised Crime.

43. Officials consider that offending that may result in four years in jail is sufficiently serious to warrant inclusion in the AISA. In the current sharing of information with the

Police, the seriousness of crimes investigated are relevant and justify a request for information from Inland Revenue.⁷

44. The Customs offences that meet the four-year threshold are of significant gravity and carry penalties that are between five years and life imprisonment. For example: importing, exporting or possessing for supply, controlled drugs⁸; knowingly importing or exporting objectionable publications⁹; money laundering¹⁰; and defrauding Customs revenue¹¹. All the offences considered by the Serious Fraud Office carry maximum terms of imprisonment of at least seven years and involve the most serious forms of financial crime.

Protecting innocent third parties' information

45. The Law Society thinks that innocent third parties may be affected by the information sharing and their interests should be protected.

46. There are already protections in place, as for every information request, the relevance of obtaining information about linked parties needs to be justified. The 'test for sharing' (in paragraph 14) is strict and must be applied before any information can be shared (proactively or on request).

47. Third-party information is not disclosed unless it is relevant to the serious crime being investigated. At the stage the information is legally reviewed prior to being disclosed, it would be determined if the information is not relevant and, in that case, it would be removed or redacted. However, with some documents, such as bank statements, it is not possible to redact every other party or joint owner of the bank account, as the context would be lost. Any information that is exchanged and is subsequently found not to be relevant, or no longer required, must be deleted within 90 days of the decision being made that the information is not required under the terms of the AISA.

48. Officials propose to clarify in the AISA that the interests of third parties should be protected as much as possible, including by deleting irrelevant information.

Sharing information about victims

49. CAANZ considers that it is not appropriate to share information about a victim without their consent, and that would be a serious breach of privacy of the victim. They recommend that a victim's consent should be sought before their personal information is shared.

50. Officials note that the 'test for sharing' is applied to ensure the information is relevant to the investigation and check 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), the victim is not usually 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). Although officials appreciate CAANZ's concern, it is impractical to obtain consent from all victims.

⁷ Inland Revenue officials analysed the cases where information was sent to the Police within a period of 12 months. All cases carried a sentence period above 4 years to life imprisonment, for crimes ranging from drugs, money laundering, fraud and violence, thus confirming the intent of sharing for truly serious crime.

⁸ Misuse of Drugs Act 1975, section 6.

⁹ Customs and Excise Act 2018, section 390.

¹⁰ Crimes Act 1961, section 243.

¹¹ Customs and Excise Act 2018, section 371.

Expertise of the Inland Revenue team managing the proactive disclosures

51. CAANZ is concerned that Inland Revenue 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 offences). They recommend that the person authorising the proactive information-sharing has the necessary skills and expertise and, in case of doubt, that the decision is reviewed by an independent person not from Inland Revenue.

52. Officials note that the information sharing is managed by a small dedicated team comprising experienced investigators with specialised training to handle such requests. Directing all shared information through a specific team ensures consistency in decision making, and that information-sharing decisions are being made by specifically trained staff.

53. Information needs to fit the criteria for sharing, and is proactively shared only when the relevance to other agencies is clearly identified – in this case, the team would only proactively share information they came across during their normal activities, and would not proactively search for information to provide to other agencies. After the information is prepared for sharing, the decision to share the information is reviewed and approved by Inland Revenue’s legal team before the information is released.

Consultation

54. The following agencies have been consulted during the development of this AISA:

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

55. The New Zealand Police has been consulted and agrees with the content of the Cabinet paper.

56. The Privacy Commissioner has reviewed the AISA and considers that the AISA meets the requirements of the Privacy Act. A copy of his submission is attached to this paper (appendix C).

Next steps

57. If you agree with the recommendations to progress this proposal, officials recommend that Ministers sign the attached Cabinet paper for referral to the Cabinet Social Wellbeing Committee for their approval. If Cabinet approval is obtained, officials will finalise the AISA and prepare a draft Order in Council to give effect to the AISA. The required legislation changes will be included in the next Taxation Bill, to apply from a date to be determined by Order in Council.

58. Subject to approval, the timeframe to complete the agreement would be in the first half of 2020, and may be fully operational before the end of 2020.

Appendices

59. The following documents are attached to this paper:
- A. Submission from the Chartered Accountants Australia and New Zealand (CAANZ)
 - B. Submission from the New Zealand Law Society (NZLS)
 - C. Privacy Commissioner - Section 96O response.

Targeting serious crime: extending information sharing

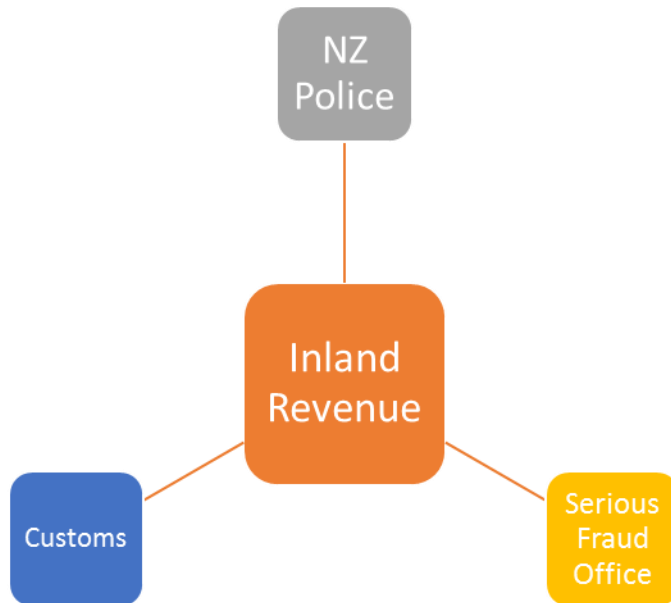
A Discussion Document

30 October 2018



Contents

- Introduction 3
- Executive Summary 4
 - Recommendations: 4
- Background 5
 - Examples of information Inland Revenue may share..... 6
 - Proactive disclosures..... 7
 - Recommendation 7
- Sharing information about victims and associated persons 8
 - Recommendation 8



Introduction

Targeting serious crime: extending information sharing

C/- Deputy Commissioner, Policy and Strategy

Inland Revenue Department

PO Box 2198

Wellington 6140

By email: policy.webmaster@ird.govt.nz

Chartered Accountants Australia and New Zealand (CA ANZ) appreciates the opportunity to provide feedback on the discussion document “Targeting serious crime: extending information sharing”.

Chartered Accountants Australia and New Zealand

We are a professional body of over 117,000 Chartered Accountants around the world. We focus on the education and lifelong learning of our members, and on advocacy and thought leadership in areas of public interest and business.

General Position

In formulating its submissions, CA ANZ takes a best practice, public policy perspective. That is, we endeavour to provide comment on a “what is best for New Zealand” basis.

We recognise Government’s legitimate right to set policy direction. We comment on those policies, and also make comment on their practical implementation. Our public policy perspective means we endeavour to provide comment free from self-interest or sectorial bias.

Executive Summary

CA ANZ understands and supports Government's desire to reduce serious crime in an efficient and effective manner. We support the initiative for the Information Sharing Agreement between Inland Revenue and the New Zealand Police ("NZ Police") to be extended to include the Serious Fraud Office ("SFO") and New Zealand Customs Service ("Customs").

However, the approved information sharing agreement does raise the following concerns:

1. that Inland Revenue will be making decisions to pro-actively share information with SFO or Customs when Inland Revenue Officers do not have the necessary skills or expertise to establish that a serious crime has been or is being or will be committed.
2. there are a lack of safeguards for taxpayers who are not suspected criminal offenders (e.g. associates or victims).

Recommendations:

- To ensure all decisions by Inland Revenue to pro-actively share information are appropriate we recommend:
 - the delegated person, who authorises the pro-active sharing of information, has the necessary skills and expertise; and
 - if there is any doubt, the decision be reviewed by an independent person.
- A victim's consent should be sought before their personal information is shared.

We are happy to discuss our submission further, and any questions can be addressed to john.cuthbertson@charteredaccountantsanz.com.

Yours Sincerely,



John Cuthbertson, CA
NZ Tax & Financial Services Leader

Background

The Government proposes to extend the existing information sharing agreement between Inland Revenue and the NZ Police to include the SFO and Customs.

Extending the existing agreement should help SFO and Customs:

- identify, investigate and prosecute fraud, corruption and cross border crime;
- improve the effectiveness and efficiencies of the services they provide;
- enable these agencies and the NZ Police to work together and provide an all of-government response to serious crime.

The existing framework and criteria that allows the NZ Police to request information from Inland Revenue or for Inland Revenue to proactively provide information to NZ Police will also apply to information sharing with the SFO and Customs.

Examples of information Inland Revenue may share

Information Inland Revenue holds on a specified person

Their IRD number, entity information, the taxes for which they are registered, income history, tax payment history (including any compliance issues), types of income, expenses, asset and liability information, and actions taken or planned to be taken in relation to the specified person. The information provided may relate to a victim of a serious offence rather than the perpetrator of the offence in order to identify a person who may have had a motive to harm the victim.

Information Inland Revenue holds on other persons or entities that are associated with, or related to, the specified person

Information necessary to understand beneficial ownership, or the nature of the structures the specified person is involved with.

Information Inland Revenue holds that is aggregated, derived or inferred that is relevant to the specified person (or associated or related persons)

Judgements about compliance behaviour and judgements on possible approaches by the specified person to compliance with tax and other legal obligations. Information shared would include documents Inland Revenue may have that would support another agency's enforcement action.

Proactive disclosures

The existing agreement allows Inland Revenue to make a proactive disclosure of information when it has reasonable grounds to suspect the information it holds is relevant to the prevention, detection or investigation of, or is evidence of a serious offence that has been committed, is being committed or will be committed. This is a very broad power.

A serious crime is broadly an offence that is punishable by imprisonment of four years or more. New Zealand's statutes include numerous categories of serious offence. Inland Revenue is likely to have some experience and expertise in suspecting or detecting offences in some categories, e.g. offences that are financial in nature. However, we are concerned that in areas outside Inland Revenue's area of responsibilities (e.g. smuggling or drug offences) Inland Revenue officers do not have the appropriate experience or expertise (nor would we expect them to have) to correctly identify possible criminal offences.

Recommendation

- To ensure all decisions by Inland Revenue to pro-actively share information are appropriate we recommend:
 - the delegated person, who authorises the pro-active sharing of information, has the necessary skills and expertise; and
 - if there is any doubt, the decision be reviewed by an independent person.

Sharing information about victims and associated persons

In addition to sharing information about the “offender”, sharing information extends to:

- organisations, entities and individuals that may be connected to the serious crime;
- individuals with whom the “offender” is related or associated
- a victim.

We do not consider it is appropriate to share information about the victim without their consent. It would be a serious breach of the privacy of the victim. It could place the victim in harm’s way and lead to unwarranted consequences.

Recommendation

- A victim’s consent should be sought before their personal information is shared.

Submission from the New Zealand Law Society

The New Zealand Law Society's submission on the *Targeting serious crime: extending information sharing* discussion document dated 2 November 2018 is available on their website at https://www.lawsociety.org.nz/_data/assets/pdf_file/0020/128423/I-IRD-information-sharing-Customs-SFO-2-11-18.pdf

Privacy Commissioner – section 960 response

See document 4 of the information release.

In Confidence

Office of the Minister of Revenue and Minister Responsible for the Serious Fraud Office

Office of the Minister of Customs

Chair, Cabinet Social Wellbeing Committee

Extending the Serious Crime Information Sharing Agreement consultation: Summary of submissions

Proposal

- 1 We propose that the Serious Fraud Office and the New Zealand Customs Service (Customs) become part of the existing Approved Information Sharing Agreement for tackling serious crime¹ (Serious Crime AISA) between Inland Revenue and the New Zealand Police (Police). The agreement extension, made pursuant to the Privacy Act 1993 (Privacy Act), would allow extending the sharing of information from Inland Revenue to these two agencies.

Executive Summary

- 2 An AISA between Inland Revenue and the Police was implemented in 2014, and has been yielding positive results in assisting with Police investigations into serious crime. The original Serious Crime AISA's framework is being proposed for extending the information sharing from Inland Revenue to the Serious Fraud Office and Customs.
- 3 An AISA is the most efficient and effective option to enable the information sharing, as it can provide increased efficiency and improved outcomes for investigations. The AISA's framework for the proposed information sharing takes into account any potential impacts on individual's privacy. The Office of the Privacy Commissioner supports this proposal to extend the existing Serious Crime AISA.
- 4 Including the Serious Fraud Office and Customs in the Serious Crime AISA would enable these agencies to receive information from Inland Revenue to help them with investigating fraud, corruption and cross-border offences that fit the "serious crime" definition. The current AISA framework would provide the mechanism to enable information sharing, while also providing robust privacy safeguards.
- 5 Inland Revenue released a discussion document and a draft AISA for public consultation at the end of September 2018. Two submissions were received, and the concerns raised were considered by officials. The draft AISA has been amended to address some of those concerns.

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

Background

- 6 The effective administration of the tax system relies heavily on voluntary compliance, for which taxpayers' trust is essential. It is critical that taxpayers trust their information will not be disclosed inappropriately.
- 7 The confidentiality rules in the Tax Administration Act 1994 (TAA) mean that Inland Revenue is not permitted to share a taxpayer's information with other agencies. However, it has been recognised that the duty to maintain confidentiality cannot be absolute, and must be balanced against the benefits to society that may be derived from disclosing information in certain, limited cases.
- 8 For this reason, there are exceptions that permit information to be disclosed for carrying into effect the Inland Revenue Acts, where the privacy of individuals has been considered and balanced against the need for government agencies to provide efficient, high-quality services, and the benefits this may generate for society.
- 9 Inland Revenue considers that the benefits to society of sharing specific information to combat serious criminal activity, where criteria are satisfied, outweigh the reduction in privacy of certain individuals and the risks to the voluntary compliance model on which the tax system is based.

Approved Information-Sharing Agreements

- 10 An AISA is a legal mechanism under the Privacy Act, which authorises the sharing of personal information between or within agencies for delivering efficient and effective public services. An AISA provides certainty on the purpose of the information sharing, the use of the information shared, and management of privacy risks. When justified, an AISA can modify the Information Privacy Principles set out in the Privacy Act. Additionally, an AISA can be amended more easily than legislation, providing a more future-proof framework for sharing information.
- 11 The development of an AISA includes consultation with the parties involved, including government agencies and persons or organisations representing the interests of the individuals whose information will be shared. This process involves continuous oversight from, and consultation with, the Privacy Commissioner. An AISA ultimately requires an Order in Council, the associated Ministerial and Cabinet approvals, and regulatory impact analysis.

The Serious Crime AISA

- 12 An AISA between Inland Revenue and the Police was implemented in 2014 to assist investigations into serious crime in New Zealand.
- 13 Under the current AISA, Inland Revenue provides information to the Police (proactively or on request) where it is relevant to the serious offence being investigated and meets the criteria for disclosure. The Police can request a range of information from Inland Revenue, which includes non-individual and individual information about tax returns, debt and audit history, and information about individuals who are linked to them.
- 14 Since its implementation, the AISA has facilitated Police investigations into serious crime. Table 1 (below) shows the results of the AISA for Inland Revenue's supply of information for prevention, detection, investigation or providing evidence of serious crime, for the last three years. The table shows an increase in the number of

investigations and prosecutions, which corresponds to the increase in information sharing from Inland Revenue to the Police.

Table1. Serious Crime AISA reporting (years 2016 to 2018)²

Year ending 30 June		2015–16	2016–17	2017–18
Number of times information was sent to the Police		112	169	222
Number of times information provided has been used in a case with a resolution of:	Prosecution	31	34	70
	Still under investigation at time of reporting	68	96	113
Estimated cost of the sharing agreement		\$10,900	\$19,995	\$9,500

Comment

- 15 Information sharing between agencies for tackling serious crime is expected to help make communities safer and reduce crime.
- 16 Options to enable efficient information sharing with the Serious Fraud Office and Customs have been assessed and discussed with the Office of the Privacy Commissioner. Extending the AISA between Inland Revenue and the Police to include these agencies is considered the best legislative option. A regulatory impact analysis is attached to this paper.
- 17 Under the proposed extension to the Serious Crime AISA, Inland Revenue would share information that could provide the Serious Fraud Office and Customs with clearer pictures of legitimate revenue streams and illegitimate money, linking individuals and businesses that might be involved in criminal activity. This would enable the Serious Fraud Office and Customs to carry out more thorough investigations, and assist these agencies to investigate a broader range of serious offences.
- 18 The same framework used for the original Serious Crime AISA would be applied to extending information sharing to the Serious Fraud Office and Customs. Inland Revenue would share information with each agency to identify, investigate and prosecute serious crime, and the sharing of information must meet a set of criteria (the 'test for sharing' framework explained below).
- 19 The information that Inland Revenue may share with Customs and the Serious Fraud Office falls into the same categories of information that Inland Revenue currently shares with the Police. It includes information on organisations, entities and individuals such as tax and financial information, information about assets, employment and social assistance, domestic and financial relationship, associates' information, and any other

² Inland Revenue Annual Report for years 2016, 2017 and 2018.

information that may be discovered by Inland Revenue while carrying out its usual functions and duties.

- 20 The existing sharing of information between Inland Revenue and the Police would remain unchanged by the addition of two further agencies to the existing AISA. The rules that currently apply to the current agreement would also apply to the proposed extension.

The “test for sharing” framework

- 21 The “test for sharing” framework would permit an agency to request, or Inland Revenue to proactively provide, information when:

- there are reasonable grounds for suspecting that a serious crime has been committed, is being committed or will be committed;
- the agency considers that there are reasonable grounds for suspecting the information is relevant to the prevention, detection, investigation, or providing evidence of a serious crime; and
- Inland Revenue is satisfied that the information is readily available within Inland Revenue, and that it is reasonable, proportionate, practicable and in the public interest to communicate the information.

The information flows

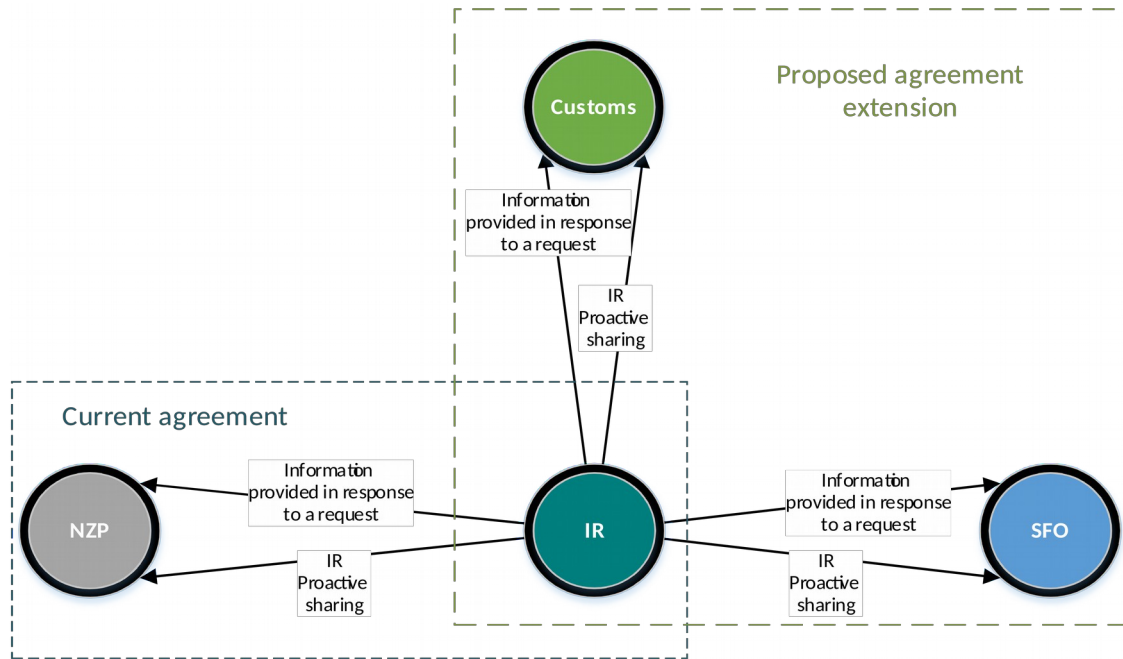
- 22 Under the current Serious Crime AISA, Inland Revenue provides information to the Police in a one-way flow of information, either proactively or in response to a request. Under the proposed AISA extension, the information flows between Inland Revenue and the Serious Fraud Office, and between Inland Revenue and Customs, would follow the same model. Information would be shared by Inland Revenue to those agencies either in response to a request or proactively.

- 23 The provision of information from the other participating agencies to Inland Revenue relies on one of the exceptions to Information Privacy Principle 11 of the Privacy Act³, and therefore has not been specifically provided for in the original AISA or the proposed extension. The Serious Fraud Office has a secrecy rule, and they will continue sharing information with Inland Revenue as authorised by one of the exceptions to their secrecy provision⁴.

- 24 The following diagram illustrates the information flows proposed in the AISA extension.

3 Information 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.

4 Serious Fraud Office Act 1990, section 36(2).



Previous public consultation and research findings

- 25 As part of the original Serious Crime AISA consultation process, submissions received from the public indicated a greater level of support for than opposition to the sharing of tax information to prevent serious crime. Submitters expressed the view that information should flow freely across government departments; that serious criminals should not be protected by privacy laws; and that more liberal sharing of information across government would result in more resources being freed up to allow an increase in the detection of people committing serious crimes.
- 26 The submissions were generally in favour of the proposals. However, the following concerns were raised as part of the original Serious Crime AISA consultation process, and were addressed by officials at the time:
- *The AISA risked undermining the integrity of the tax system.*
 - *Undue infringement upon individuals' rights and privileges.*
 - *Impact on Inland Revenue's existing powers of search and seizure.*
 - *Need for staff sufficiently experienced to make the required judgements to authorise the release of information.*
 - *Security and use of information.*
- 27 Inland Revenue often commissions research on public perception of sharing taxpayer information. Results have shown that public opinion is not affected negatively where information is shared for the right reasons between the right agencies.
- 28 Findings from recent qualitative research⁵ conducted on "information sharing and tax compliance" indicates that people support information sharing when its public good is

⁵ ThinkPlace, Information Sharing and Tax Compliance, How might people change their behaviour?, July 2018

clear. Sharing information for the public good supports trust in the government, and aligns with the motivations for compliance of those interviewed as part of the research.

Discussion of submissions from public consultation

- 29 Consultation is a key part of the AISA development process, and a requirement under the Privacy Act.⁶ The agencies involved in the AISA must consult with the government agencies and persons or organisations that represent the interests of the parties involved, including the individuals whose information is to be shared. The Office of the Privacy Commissioner oversees the process and provides input into the agreement.
- 30 Public consultation was undertaken from 26 September to 30 October 2018. The discussion document *Targeting Serious Crime: extending information sharing*, outlining the sharing process in detail, and the draft AISA document, were made available to the public.
- 31 Two submissions were received in this round of consultation. The Chartered Accountants Australia and New Zealand (CAANZ) supports the proposal and provided recommendations, and the New Zealand Law Society (Law Society) has concerns with the proposed agreement extension. Submitters raised similar concerns to those raised about the original Serious Crime AISA in 2013.
- 32 The Law Society claims that there has been an erosion in confidentiality by the introduction of exceptions and is concerned that the AISA risks undermining the integrity of the tax system by sharing information (originally collected for tax purposes) for purposes that are not strictly tax-related. Therefore, they consider that Inland Revenue's collection powers should be revisited to consider if there should be, as a consequence, a corresponding decrease in those powers.
- 33 Inland Revenue acknowledges that many exceptions to confidentiality have been introduced into the Tax Administration Act 1994 (TAA) over the years, and this has generally not been associated with discussions about its information gathering powers. The approach to information-sharing has changed over time to reflect modern expectations of transparency and efficient government administration, and the confidentiality exceptions, initially introduced to facilitate the performance of tax-related functions, are currently aiming to achieve wider public policy goals.
- 34 Research indicates that the public generally approve of sharing that benefits society, either by facilitating the provision of public services or helping to uphold the law. Research does not show that there is likely to be a significant impact on voluntary compliance, or that Inland Revenue's information-gathering powers should be restricted as a result.
- 35 The Law Society is concerned that the AISA unduly infringes a taxpayer's right to be free from unreasonable search and seizure, and the privilege against self-incrimination. They believe that the agencies receiving information from Inland Revenue would be taking advantage of Inland Revenue's coercive powers to obtain information that they would not be able to obtain otherwise and, as a result, this is a breach of section 21 of the Bill of Rights Act 1990⁷ (NZBoRA), which prohibits unreasonable search and seizure.

⁶ Privacy Act 1993, s 96O.

⁷ Section 21 - Unreasonable search and seizure - Everyone has the right to be secure against unreasonable search or seizure, whether of the person, property, or correspondence or otherwise.

- 36 Officials believe that, to the extent that the AISA extension imposes limits on taxpayers' rights, these constitute reasonable limitations in terms of section 5 of the NZBoRA⁸. Inland Revenue will not exercise its powers to collect information on behalf of the other agencies or share personal information that is not already readily available within Inland Revenue.
- 37 Regarding the privilege against self-incrimination, information obtained under compulsion under sections 17I and 17J of the TAA⁹ 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 those sections would not be shared, unless the other agency has the same power to obtain that information.
- 38 The recent changes made to the TAA have taken the approach that Inland Revenue will be required to consider the provenance of information and whether any particular security arrangements are needed, rather than including a blanket prohibition on sharing information obtained by compulsion. For this AISA, the same approach has been adopted in relation to the on-sharing of information obtained under coercive powers (sections 17 and 17B of the TAA¹⁰).
- 39 Officials consider this is a reasonable approach, as a blanket restriction on sharing such information has not been included in the TAA, and the Privacy Act 1993 does not contain any provisions that would limit the sharing of such information in the context of the Approved Information Sharing Agreement (AISA) regime.
- 40 The Law Society considers that the serious crime definition threshold was set at too low a level and would result in the sharing of information concerning offences that fall short of truly serious offending.
- 41 Officials consider that offending that may result in four years in jail is sufficiently serious to warrant inclusion in the AISA. 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.
- 42 The Customs offences that meet the four-year threshold are of significant gravity and carry penalties that are between five years and life imprisonment. For example: importing, exporting or possessing for supply of controlled drugs; knowingly importing or exporting objectionable publications; money laundering; and defrauding Customs revenue. All the offences considered by the Serious Fraud Office carry maximum terms of imprisonment of at least seven years and involve the most serious forms of financial crime.
- 43 The Law Society suggested that the interests of innocent third parties who may be affected by the information sharing should be protected. Officials believe that this is already managed through the strict "test for sharing", which ensures the information to be shared is justified and relevant to the investigation. The agreement states that any

⁸ Section 5 - Justified limitations – Subject to section 4, the rights and freedoms contained in this Bill of Rights may be subject only to such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society.

⁹ Section 17I - Commissioner may conduct inquiries, and section 7J - Commissioner may apply for District Court Judge to conduct inquiries

¹⁰ Section 17 - Commissioner may obtain information by accessing property or documents, and section 7B - Commissioner may require information or production of documents [Corrected footnote for information release]

information that is not relevant or no longer required by the agency must be deleted within 90 days of the non-requirement decision being made. To add further protections, it has been included in the agreement that third parties' interests must be protected to the extent practicable.

- 44 Submissions have also raised the need to ensure transparency and include notification processes by obtaining a victim's consent, and notifying the taxpayers whose information has been obtained under compulsion.
- 45 The AISA ensures that certain criteria are met, to confirm that the information is relevant to the investigation and the intent of the sharing. In certain cases, informing and obtaining consent from a victim may prejudice the investigation and have an adverse effect, or may be impractical if there are multiple victims.
- 46 Notifying a suspected person that their information has been shared would be inappropriate as it would put the person on notice that they are under investigation. Inland Revenue's privacy statement on forms and on its website notifies taxpayers that their information may be shared with other agencies. However, officials will look at further informing taxpayers, when information is collected under compulsion, that their information may be shared with other agencies when appropriate.
- 47 CAANZ is concerned at the level of expertise of the Inland Revenue team managing the proactive disclosures on criminal matters. This concern has been expressed in a previous consultation, and has been addressed by ensuring that the team handling the information-sharing requests is an experienced, dedicated team, with specialised training. Before the information is released, it is checked and approved by Inland Revenue's legal team.

Consultation with other agencies

48 The following agencies have been consulted during the development of this AISA:

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

49 The Privacy Commissioner has reviewed the draft AISA and considers that it meets the requirements of the Privacy Act. The submission from the Privacy Commissioner is attached to this paper.

Financial Implications

50 The cost of implementing the AISA will be met from the existing financial baselines of all agencies.

System or Technology Impacts

51 For Inland Revenue, implementation impacts are minimal. The current process used to share information with the Police would also be used for disclosing information to the Serious Fraud Office, and to Customs. The same operational units would continue to handle the requests for information using their 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 mail (SeeMail).

- 52 For the Serious Fraud Office, there would be no or little implementation impact. The Serious Fraud Office is already equipped to receive, store and review information from Inland Revenue as appropriate, and would use existing channels to continue to do so.
- 53 Customs would use existing information technology systems and processes to manage information shared by Inland Revenue, with appropriate mechanisms to ensure confidentiality of taxpayer information.

Human Rights

- 54 Any limitations that the AISA extension may impose on taxpayers' rights are reasonable limits, and are in accordance with section 5 of the NZBoRA. Limitations on taxpayers' rights can be justified by the benefits of reduction in societal harm from serious crime. The participating agencies consider that the benefits of sharing information in specific cases, and within limitations, justify and outweigh the potential infringement of taxpayers' rights.
- 55 The AISA extension engages section 21 of the NZBoRA, the right to be free from unreasonable search and seizure. A request for information about an individual made by one agency to another could amount to a "search" in terms of section 21. Officials consider that the information-sharing powers in the AISA are reasonable to achieve the important objective of enabling agencies to carry out more thorough investigations into serious offences to help make communities safer and reduce crime. Officials also consider the AISA provisions are rationally connected and proportionate to this objective, as discussed in paragraphs 29 to 45.
- 56 If an information request of this type does amount to a search, the empowering provision in the Privacy Act 1993 only authorises the approval of information-sharing agreements that are consistent with section 21. Therefore, the AISA would be read in accordance with the NZBoRA.

Legislative Implications

- 57 The proposals will require an Order in Council under the Privacy Act, to bring the AISA into operation. We anticipate that the Order in Council will be submitted to Cabinet for consideration in early 2020.
- 58 The current legislative information-sharing provision between Inland Revenue and the Serious Fraud Office will need to be repealed, with effect from a future date set by Order in Council, to give effect to the AISA. This is to ensure that there is only one authorising provision in force at any point in time to enable information sharing between the two agencies.
- 59 At the same time the AISA comes into force, an Order in Council will approve the repeal of the information-sharing provision between Inland Revenue and the Serious Fraud Office.

Regulatory Impact Analysis

- 60 Regulatory impact analysis requirements apply to this paper. A regulatory impact analysis (RIA) is therefore attached to this paper.

Quality of the impact analysis

- 61 The Quality Assurance reviewer at Inland Revenue has reviewed the *Extending the Targeting Serious Crime information sharing agreement* RIA, and considers that the

information and analysis summarised in it meets the quality assurance criteria of the Regulatory Impact Analysis framework.

Gender Implications

62 There are no specific gender implications from the proposals in this paper.

Disability Perspective

63 There are no specific implications for people with disabilities associated with the proposals in this paper.

Publicity

64 We are proposing to release a media statement at the time that the Order in Council is introduced.

Proactive Release

65 We propose to proactively release this Cabinet paper, associated minutes and key advice papers in full within 30 working days of Cabinet making final decisions.

Recommendations

The Minister of Revenue and Minister Responsible for the Serious Fraud Office, and the Minister of Customs, recommend that the Committee:

1. **Note** that information sharing concerning taxpayer information may take place under Part 9A of the Privacy Act 1993 through an Order in Council using the AISA mechanism.
2. **Agree** to the preparation of the extension of the Serious Crime AISA to enable the sharing of information from Inland Revenue to the Serious Fraud Office, and to Customs.
3. **Agree** to delegate to the Minister of Revenue and Minister Responsible for the Serious Fraud Office, in conjunction with the Minister of Customs where appropriate, the authority to make decisions on the detailed implementation of these proposals.
4. **Invite** the Minister of Revenue to instruct the Parliamentary Counsel Office to prepare draft Orders in Council, which will approve the information-sharing agreement, in accordance with the Privacy Act 1993, as well as consequential Order to repeal the existing sharing provision between Inland Revenue and the Serious Fraud Office.

Authorised for lodgement

Hon Stuart Nash
Minister of Revenue and Minister Responsible for the Serious Fraud Office

Hon Jenny Salesa
Minister of Customs



Information Sharing Agreement

Between

Inland Revenue

And

**New Zealand Police, New Zealand Customs Service and
Serious Fraud Office**

Relating to

**Disclosure of information by Inland Revenue for the purpose of prevention,
detection, investigation or providing evidence of serious crime**

**Pursuant to Part 9A of the Privacy Act 1993 and section 18E(2) of the Tax
Administration Act 1994**

August 2019

Information Sharing Agreement Amendment Agreement

The Parties

Inland Revenue (IR) (acting through the Commissioner of Inland Revenue)

And

New Zealand Police (NZ Police) (acting through the Commissioner of Police)

And

New Zealand Customs Service (NZ Customs) (acting through the Comptroller of Customs)

And

Serious Fraud Office (SFO) (acting through the Director)

The Agreement

IR and NZ Police entered into an information sharing agreement on 2 July 2014 to enable IR to receive requests for Personal Information from, and to disclose Personal Information to, NZ Police for the purpose of the prevention, detection, investigation or providing evidence of Serious Crime (**Original Agreement**).

The Original Agreement was approved under the Privacy Act 1993 by Order in Council made on 26 May 2014. The Original Agreement was amended by an Amendment Agreement entered into on 16 March 2015, in anticipation of a further Order in Council made on 29 May 2015. The Original Agreement was further amended by an Amendment Agreement entered into on 21 June 2017, to enable the Parties to share non-Personal Information.

IR, NZ Police, NZ Customs and SFO agree to further amend the Original Agreement (as amended in June 2017) as shown in Schedule 1 of this agreement to add NZ Customs and SFO as Parties and, at the time of signing this agreement, to sign an original of the document set out in Schedule 2 of this agreement as a conclusive record of the Original Agreement (as amended in June 2017) with those further amendments incorporated (the **Agreement as Amended**).

The parties acknowledge that, under the Privacy Act 1993-

- (a) subject to paragraph (b) below, the Original Agreement (as amended in March 2015) will continue to have effect as if the amendments shown in Schedule 1 had not been made by this agreement; and
- (b) the Agreement as Amended will only have effect (and replace the Original Agreement, as amended in June 2017) on and from the date that it is signed by the Parties.

Acceptance

In signing this Amendment Agreement, each party acknowledges that it has read and agrees to be bound by it.

For and on behalf of **Inland Revenue:**

For and on behalf of **New Zealand Police:**

Naomi Ferguson
Commissioner
Inland Revenue

Mike Bush MNZM
Commissioner
New Zealand Police

Date: _____

Date: _____

For and on behalf of **New Zealand Customs Service:**

For and on behalf of **Serious Fraud Office:**

~~Christine Stevenson~~ ~~Bill Perry~~—
Acting Comptroller
New Zealand Customs Service

Julie Read
Director
Serious Fraud Office

Date: _____

Date: _____

Information Sharing Agreement

Between

Inland Revenue

And

**New Zealand Police, New Zealand Customs Service and
Serious Fraud Office**

Relating to

**Disclosure of information by Inland Revenue to New Zealand Police for the
purpose of prevention, detection, investigation or providing evidence of
serious crime**

**Pursuant to Part 9A of the Privacy Act 1993 and section 81A-18E(2) of the
Tax Administration Act 1994**

June 2017 August 2019

Contents

- Defined terms 8
- Background 10
- Terms 10
- 1. Objectives and purpose of the Agreement 10
- 2. Exemptions and/or modifications to information privacy principles 11
- 3. The public service or public services the provision of which the Agreement is intended to facilitate 11
- 4. Type of Information to be shared under the Agreement 11
- 5. The [pParties](#) involved and the lead agency 13
- 6. Description of Personal Information to be shared between [IR and each Participating Agencies](#) 13
- 7. How the [pParties](#) may use the Personal Information 14
- 8. Adverse actions 15
- 9. Where you can view this document 16
- 10. Overview of the operational details 16
- 11. Safeguards to protect privacy and security 17
- 12. Assistance statement 20
- 13. Security provisions 20
- 14. Dispute resolution 21
- 15. Review of the Agreement 21
- 16. Amendments to the Agreement 21
- 17. Term, performance and termination 21
- 18. Departmental representatives 22

Information Sharing Agreement

The Parties

Inland Revenue (IR) (acting through the Commissioner of Inland Revenue)

And

New Zealand Police (NZ Police) (acting through the Commissioner of Police)

And

New Zealand Customs Service (NZ Customs) (acting through the Comptroller of Customs)

And

Serious Fraud Office (SFO) (acting through the Director)

The Agreement

This Agreement is put in place under Part 9A of the Privacy Act 1993 and section ~~81A-18E(2)~~ of the Tax Administration Act 1994 to enable IR to receive requests for Information from, and to disclose Information to, ~~NZ Police~~ the Participating Agencies for the purpose of the prevention, detection, investigation or providing evidence of Serious Crime.

Acceptance

In signing this Agreement (as amended), each ~~party~~ Party acknowledges that it has read and agrees to be bound by it.

For and on behalf of **Inland Revenue**:

For and on behalf of **New Zealand Police**:

Naomi Ferguson
Commissioner
Inland Revenue

Mike Bush MNZM
Commissioner
New Zealand Police

Date: _____

Date: _____

For and on behalf of **New Zealand Customs Service:** For and on behalf of **Serious Fraud Office:**

Bill Perry
Acting Comptroller
New Zealand Customs Service

Julie Read
Director
Serious Fraud Office

Date: _____

Date: _____

Witnessed by:

Name: _____

Signature: _____

Position: _____

Date: _____

DRAFT

Defined terms

In this Agreement unless the context otherwise requires:

“**Agreement**” means this information sharing agreement, including any amendment made by the Parties.

“**Appropriately Authorised Staff**” means ~~NZ Police~~ a Participating Agency’s employees or anyone engaged by ~~NZ Police~~ Participating Agency assigned to assess, investigate or prosecute any matter or case concerning Serious Crime to which Information shared by IR under this Agreement is or may be relevant.

“**Assets**” means any real and personal property that is or was held, or in which an interest is or was held, by a Person, including cash as defined in section 2(1) of the Financial Transactions Reporting Act 1996, in bank accounts, accounts in financial institutions, shareholdings and beneficial interests in trust.

“**Associates**” mean Persons that a Person is or was connected with in an act, enterprise or business.

~~“**CIR**” means the Commissioner of Inland Revenue which has the same meaning as that term in section 3 of the Tax Administration Act 1994.~~

~~“**CNZP**” means the Commissioner of Police which has the same meaning as Commissioner in section 4 of the Policing Act 2008.~~

“**Domestic Relationship**” means a current or previous relationship between an identifiable Individual and another person who is or was a spouse or partner of the Individual, is or was a family member of the Individual or ordinarily shares or shared a household with the Individual.

“**Domestic Relationship Information**” means information about a Domestic Relationship and includes:

- (a) the current and previous names, aliases and contact details of Individuals with whom an identifiable Individual has or had a Domestic Relationship and the dates of birth of those Individuals;
- (b) information about the Assets and Liabilities of those Individuals; and
- (c) Employment Information, Social Assistance Information, Financial Transaction Information and Tax Information about those Individuals.

“**Employment Information**” includes information about: (a) an identifiable Individual’s current or previous engagement in a contract of service or a contract for service; (b) the parties to such a contract; and (c) any other Information relevant to the engagement (including contractual terms to the extent they are relevant).

“**Financial Relationship**” includes a Person's current or previous business or financial relationship with, business or financial interest in, or other business or financial link to, one or more other Persons. The connection between an Individual and: (a) a company of which they are or were a director and/or shareholder; (b) a trust of which they are or were a beneficiary and/or trustee and/or settlor; (c) a partnership of which they are or were a partner; and (d) a bank account number nominated for the Individual’s tax purposes, is included in the definition of a financial relationship.

“**Financial Relationship Information**” means information about a Financial Relationship and includes:

- (a) the current and previous names, aliases and contact details of Persons with whom a Person has or had a Financial Relationship and, in relation to Individuals, the dates of birth of those Individuals;
- (b) information about the Assets and Liabilities of those Persons;
- (c) Employment Information, Financial Transaction Information and Tax Information about or concerning those Persons.

“Financial Transaction Information” means information about a movement of Assets and Liabilities, or an agreement to move Assets and Liabilities.

“Individual” means a living or deceased natural person.

“Information” means Personal Information and any other information about a Person that may be shared under this Agreement.

~~“IR” means the Inland Revenue Department, including the Commissioner.~~

“Liabilities” means current and previous liabilities.

“MFT” means Managed File Transfer process which is a secure automated data transfer process.

~~“NZ Police” means the New Zealand Police, including the Commissioner and the vote responsibilities of the New Zealand Police.~~

“Order in Council” means the Order in Council or Orders in Council (if the context requires) made in accordance with sections 96J and 96V of the Privacy Act 1993 relating to this Agreement.

~~“Participating Agency” means NZ Police, NZ Customs or SFO and “Participating Agencies” has a corresponding meaning.~~

~~“Party” means IR, NZ Police, NZ Customs or SFO and “Parties” has a corresponding meaning.~~

“Person” includes an Individual, a corporation sole, a body corporate, and an unincorporated body, association, organisation, group, trust, partnership, board or society and Persons has a corresponding meaning.

“Personal Information” has the meaning in section 2(1) of the Privacy Act 1993.

“Person Record” means a Person’s current and previous names, aliases, trade names and contact details, and in relation to Individuals, includes their date of birth.

“Privacy Commissioner” means Office of the Privacy Commissioner.

“Secure Electronic Environment Mail (SEEMail)” means a secure government email service, the environment for which is formed by a group of participating agencies that use accredited secure email gateways that sign and encrypt sensitive messages sent between them using Secure Multipurpose Internet Mail Extension (S/MIME) technologies.

~~“Secure Transmission Method” means a secure online file transfer, SEEMail, Ironkey or other secure means of transmitting information which:~~

- (a) ~~in relation to the transfer of “Restricted” information (as defined in the current New Zealand Government Security Classification System), is consistent with the standards (including encryption measures) in the current New Zealand Information Security Manual (NZISM) or its equivalent; and~~

(b) in relation to the transfer of other information that is not restricted, the Parties will make reasonable efforts to ensure is consistent with those standards.

“**Serious Crime**” means an offence punishable by imprisonment of four years or more.

“**Social Assistance**” means child support, student loan or Working for Families.

“**Social Assistance Information**” means information about an Individual's current and previous Social Assistance status, entitlement, debt, Liabilities, payments and balance.

“**TAA**” means the Tax Administration Act 1994.

“**Tax Information**” includes information about a Person’s current and previous tax affairs, tax class, income, tax paid, tax refunds, tax adjustments, and Liabilities ~~and~~.

Unless otherwise defined above, terms defined in sections 2, 96C and 97 of the Privacy Act 1993 shall have the same meaning in this Agreement as they do in that Act.

Background

The Government has set out its commitment to reforms that ensure the public sector takes a more collaborative, cross-agency approach to supporting New Zealanders and gaining efficiencies. A key part of this commitment ~~includes is~~ reducing the rates of crime. It has been identified that sharing information between ~~IR and the NZ Police~~ IR and a Participating Agency is would be one way of supporting these goals.

The tax secrecy rules in the TAA prevent IR from sharing information with other agencies other than when a specified exception applies. One exception to tax secrecy is that Information may be shared when in accordance with an approved information sharing agreement pursuant to Part 9A of the Privacy Act 1993.

This Agreement has been put in place under Part 9A to enable IR to share Information with ~~NZ Police~~ the Participating Agencies, for the purpose of detection, prevention, investigation or providing evidence of Serious Crime. IR may share Information with ~~NZ Police~~ one or more Participating Agency either proactively or in response to a request from ~~NZ Police~~ a Participating Agency. That Information may relate to Persons that may be involved in or otherwise connected to a Serious Crime as well as Persons with whom they have or have had a relationship (for example, family members or Associates).

This Agreement cannot and does not purport to override any provisions in any enactment other than any part of the Privacy Act 1993 as authorised pursuant to Part 9A of that Act.

Terms

1. Objectives and purpose of the Agreement

Objectives

The objectives of this Agreement are to:

- (a) Prevent and reduce the level of Serious Crime ~~committed~~;
- (b) Gain efficiencies through more collaborative, cross-agency work; and
- (c) Enable sufficient protection of people’s privacy and ensure a proper level of security and transparency.

Objectives (a) and (b) can potentially conflict with objective (c), if robust ~~security systems and~~ [privacy processes and practices](#) are not established to protect people's privacy. To ensure that a potential conflict is managed appropriately a balance between providing better public services and ensuring that peoples' information is adequately protected is required.

Purpose

The purpose of this Agreement is to enable IR to share Information with ~~NZ Police~~ [the Participating Agencies](#) for the purposes of prevention, detection, investigation or providing evidence of a Serious Crime that there are reasonable grounds to suspect has been committed, is being committed, or will be committed. IR may share Information with ~~NZ Police~~ [the Participating Agencies](#) either in response to a request from ~~NZ Police~~ [a Participating Agency](#) or proactively.

The Agreement does not cover information sharing as part of the Criminal Proceeds (Recovery) Act 2009. Nothing in this Agreement affects that Act.

2. Exemptions and/or modifications to information privacy principles

For the purposes of this Agreement information privacy principles 2 and 11 which are set out in section 6 of the Privacy Act 1993 are modified (by the Order in Council) as follows:

Principle 2: Source of Personal Information

It is not a breach of information privacy principle 2 for IR to collect Personal Information from ~~NZ Police~~ [the Participating Agencies](#) or ~~NZ Police~~ [for the Participating Agencies](#) to collect Personal Information from IR for the purposes of this Agreement.

Principle 11: Limits on disclosure of personal information

It is not a breach of information privacy principle 11 for ~~NZ Police~~ [the Participating Agencies](#) to request Personal Information from IR (which itself may entail the disclosure of Personal Information to IR) or for IR to provide Personal Information to ~~NZ Police~~ [the Participating Agencies](#) for the purposes of this Agreement.

[When IR collects information from individuals, either voluntarily or by compulsion, they are notified that the information that they provide to IR may be shared with other government agencies who are entitled to the information under legislation.](#)

3. The public service or public services the provision of which the Agreement is intended to facilitate

The public services that this Agreement is intended to facilitate are maintaining public safety, law enforcement and crime prevention. In particular, this Agreement is intended to facilitate the provision of Information for the prevention, detection or investigation of, or as evidence of, Serious Crime. This may result in the prosecution of a Person for a Serious Crime.

4. Type of Information to be shared under the Agreement

Test for sharing

Information sharing under this Agreement will only occur where [either of](#) the following tests [are is](#) met:

~~NZ Police~~A Participating Agency may request Information from IR and IR may share Information with ~~NZ Police~~A Participating Agency in response to that request, ~~or IR may proactively share Information with NZ Police~~A Participating Agency, where:

- ~~NZ Police~~A Participating Agency (if requesting) or IR (if proactively sharing) has reasonable grounds to suspect that a Serious Crime has been, is being, or will be, committed; and
- ~~NZ Police~~A Participating Agency (if requesting) or IR (if proactively sharing) has reasonable grounds to suspect that the Information is relevant to the prevention, detection or investigation of, or is evidence of, a Serious Crime and confirms that it reasonably believes that the amount of Information requested is reasonable and proportionate for those purposes, in the circumstances; and
- A Participating Agency has taken all reasonable steps to obtain the Information from other sources without success (where practicable); and
- IR determines that the Information is readily available within IR and verifies that it is reasonable, proportionate, practicable and in the public interest to provide the Information to ~~NZ Police~~the Participating Agency.

IR may proactively share Information with a Participating Agency, where:

- IR has reasonable grounds to suspect that a Serious Crime has been, is being, or will be, committed; and
- IR has reasonable grounds to suspect that the Information is relevant to the prevention, detection or investigation of, or is evidence of, a Serious Crime; and
- IR determines that the Information is readily available within IR and verifies that it is reasonable, proportionate, practicable and in the public interest to provide the Information to the Participating Agency.

As noted above, this Information may relate to Persons that may be involved in or otherwise connected to a Serious Crime as well as Persons with whom they have or have had a relationship (for example, family members or Associates). Participating Agencies will use reasonable endeavours to protect the interests of Persons who are indirectly connected to a Serious Crime, or related to a Person who is involved in or otherwise connected to a Serious Crime, including by destroying any information that is not relevant or no longer required in accordance with this Agreement and, where appropriate, by redacting third party information from information given in evidence.

The Information may relate to such offending as, for example, investor fraud, money laundering or drug manufacturing or distribution. This is an indicative list only for the purposes of illustration. When sharing with the NZ Police and NZ Customs, it will not include Information that IR has obtained by compulsion using its powers under sections 17I and 17J of the TAA. However, SFO may request any such Information, provided that (in addition to confirming that the relevant test for sharing above is met) the SFO confirms that there are reasonable grounds to believe that an offence involving serious or complex fraud may have been committed. Before sharing Information that IR has obtained by compulsion under sections 17 or 17B of the TAA, IR will determine whether particular conditions are required to be specified for the security and use of that Information.

For the avoidance of doubt, subject to the “Disclosure” provisions of clause 11, a Participating Agency may proactively share information that it holds in relation to Serious Crime with IR or another Participating Agency in accordance with relevant provisions of legislation that it administers (such as

[section 36 of the Serious Fraud Office Act 1990\) or the information privacy principles contained in section 6 of the Privacy Act 1993.](#)

5. The ~~parties~~ Parties involved and the lead agency

As indicated above, this Agreement is between [IR and the Participating Agencies, namely NZ Police, NZ Customs, SFO and IR](#). IR is the lead agency.

6. Description of information to be shared between ~~the Parties~~ IR and each Participating Agency

IR will only share Information with [NZ Police a Participating Agency](#) where the [relevant](#) test for sharing in clause 4 above has been met.

~~NZ Police~~ [A Participating Agency](#) may request that IR share ~~information~~ Information falling within the categories in Row 1 of the table below and IR may share such ~~information~~ Information in response to a request. In making such a request of IR, ~~NZ Police~~ [A Participating Agency](#) may itself need to share ~~certain information (such as identifying details~~ Person Records and grounds for the request) with IR, to enable IR to process the request and/or for IR to assess whether relevant parts of the test are met.

IR may proactively share ~~information~~ Information described in Row 2 of the table below. This means that IR may proactively share ~~information~~ Information that could otherwise be requested by [NZ Police a Participating Agency](#) under Row 1, and any other ~~information~~ Information discovered by IR in the course of carrying out its usual functions and duties (however discovered) with [NZ Police a Participating Agency](#) when the test is met.

The information that IR may share with [NZ Police a Participating Agency](#) can include:

<p>Row 1</p>	<p>Information IR may share with NZ Police a Participating Agency upon request</p>	<ul style="list-style-type: none"> • Information about a Person's Associates • Tax Information • Financial Transaction Information • Financial Relationship Information • Domestic Relationship information • Information about Assets • Employment Information • Person Records • Social Assistance Information
<p>Row 2</p>	<p>Information IR may share with NZ Police a Participating Agency proactively</p>	<ul style="list-style-type: none"> • Information falling within the categories in Row 1 above • Any other Information discovered by IR in the course of carrying out its

		usual functions and duties (however discovered)
--	--	--

For the avoidance of doubt, IR may share both current and previous information, as held by IR, with [NZ Police Participating Agency](#).

7. How the ~~parties~~ Parties may use the Information

IR may use Information received from [NZ Police Participating Agency](#) under this Agreement to process an ~~an NZ Police Participating Agency~~ request and/or to assess whether relevant parts of the test in clause 4 above are met.

~~NZ Police~~ [A Participating Agency](#) may use Information received under this Agreement for the purpose of prevention, detection or investigation of, or to use as evidence of, a Serious Crime (subject to section 17K of the TAA, which provides that statements made by a person in answer to a question put to them in the context of an inquiry under section 17I or 17J of the TAA are not admissible in criminal proceedings against the person, except on a charge of perjury). This may involve undertaking the following types of activities (note that this is an indicative list only for the purposes of illustration):

- Identifying the commission or potential commission of a Serious Crime.
- Identifying individuals involved in a Serious Crime (e.g., victims, offenders, witnesses).
- Identifying other lines of inquiry for a Serious Crime.
- Using the Information as intelligence for a Serious Crime investigation.
- Using the Information as evidence in the investigation and prosecution of any Person for a Serious Crime.
- Using the Information as part of an investigation into a Serious Crime to identify roles and relationships within criminal networks to then identify the enablers of financial structures.
- Identifying potential victims or offenders of Serious Crimes to enable activation of preventative measures.
- Enabling, where the test is met, the sharing of Information for joint ~~NZ Police~~ [Participating Agency](#) and IR taskforces.

Information used in any of the respects above may also be turned into anonymised data for the purpose of producing strategic intelligence products that detail crime trends.

~~Neither p~~ [No Participating Agency](#) will use any Information shared under this Agreement for any purpose other than as set out in this Agreement. For example, ~~IR will not use Information received from NZ Police under this Agreement for TAA purposes and NZ Police~~ [Participating Agency](#) will not use Information received under this Agreement:

- ~~As evidence of a non-serious crime that is not a Serious Crime;~~ [or](#)
- [For conducting data analytics; or](#)

- As general intelligence information-: [or](#)
- As part of a vetting process.

These restrictions do not apply from the point in time (if any) that the Information becomes publicly available as a result of legitimate public disclosure or as a result of court proceedings.

8. Adverse actions

Section 96Q of the Privacy Act 1993 requires agencies to provide written notice to individuals before any “adverse action” is taken against them on the basis of Personal Information shared under an information sharing agreement, and give those individuals 10 working days to dispute the information received.

Section 96R allows agencies to either dispense with the requirements under section 96Q or [to](#) shorten the 10 working day period.

Information (including Personal Information) held by IR will only be shared with [NZ Policea Participating Agency](#) where there are reasonable grounds to suspect that a Serious Crime has been committed, is being committed or will be committed and that the Information is relevant to the prevention, detection, investigation or the provision of evidence of a Serious Crime. Much of [NZ Police’sa Participating Agency’s](#) early assessment and investigative work is sensitive. Advance notification by [NZ Policea Participating Agency](#) of an adverse action would ‘tip off’ an alleged serious criminal offender.

For these reasons [NZ Policethe Participating Agencies](#) will dispense with the notice requirements under section 96Q for this Agreement.

To the extent that IR’s use of Personal Information received from [NZ Policea Participating Agency](#) to locate Information (including Personal Information) held by IR for disclosure to [NZ Policea Participating Agency](#), or IR’s sharing of Information with [NZ Policea Participating Agency](#), could be considered an adverse action, IR will dispense with the notice requirement under section 96Q for this Agreement.

Adverse actions [NZ Policea Participating Agency](#) may take

The type of adverse action [NZ Policea Participating Agency](#) may take is dependent on:

- the nature of the Serious Crime and the immediacy of action required e.g., a homicide versus a financial crime; and
- the nature and value of Information when considered alongside the facts of a case and material held by [NZ Policethe Participating Agency](#).

The types of adverse action could include (but are not limited to):

- investigation;
- arrest; and
- prosecution.

[NZ PoliceA Participating Agency](#) may also use its range of statutory powers to support the exercise of these actions.

[NZ PoliceA Participating Agency’s](#) employees or anyone engaged by [NZ Policethe Participating Agency](#) will comply with all [NZ Policeof the Participating Agency’s](#) policies and guidelines as well as

the Solicitor General's Prosecution Guidelines (Guidelines), before taking any adverse action. The Guidelines assist in determining:

- whether criminal proceedings should be commenced;
- what charges should be filed; and
- whether, if commenced, criminal proceedings should be continued or discontinued.

The Guidelines also provide advice for the conduct of criminal prosecutions, and establish standards of conduct and practice expected from those whose duties include conducting prosecutions.

If Information shared under this Agreement forms part of the prosecution's evidence in a criminal case, the Information may be disclosed to an individual in accordance with the Criminal Disclosure Act 2008. Any dispute about the provision of such information will be managed by the courts as part of the subject matter of the prosecution.

IR and adverse actions

Except to the extent that IR's locating and sharing of Personal Information with [NZ Policea Participating Agency](#) could be considered adverse action, IR will take no adverse actions [under this Agreement](#) as a result of receiving Personal Information from [NZ Policea Participating Agency](#) under this Agreement.

9. Where you can view this document

This document is available [to the public online at www.ird.govt.nz and www.police.govt.nz or at on the public website of each Party or in person at:](#)

Inland Revenue
Asteron Centre
Level 5
55 Featherston Street
Wellington 6011

10. Overview of the operational details

Requests for Information by [NZ Policea Participating Agency](#) will be passed to and managed by a designated team in [NZ Policee the Participating Agency](#). They will decide whether the parts of the test in clause 4 required to be satisfied by [NZ Policee the Participating Agency](#) are met and whether the request should be sent to IR. Requests for Information will be sent to a particular nominated team at IR. Certain staff members will ascertain whether IR holds the Information sought and decide whether that Information may be released to [NZ Policee the Participating Agency](#), having applied the relevant parts of the test.

In the case of proactive release of Information by IR to [NZ Policea Participating Agency](#), IR personnel will pass the Information to be considered for proactive release to the same nominated IR team so that a decision can be made as to whether the Information can be provided to [NZ Policee the Participating Agency](#) in accordance with the test.

Senior personnel within each [agency-Party](#) will be responsible for the relevant decision-making by [their agencythat Party](#). From NZ Police this will be overseen by the Manager: Intelligence Operations (or their nominated Deputy), based in the National Intelligence Centre, or relevant successor personnel. From IR this will be overseen by the Manager: Investigations (or their nominated Deputy), or relevant successor personnel. [From NZ Customs this will be overseen by the Manager: Intelligence \(or their nominated Deputy\). From SFO this will be overseen by the General Counsel.](#)

Subject to the commentary below, [IR and NZ Policee the Parties](#) will use [the SEEMail environmenta Secure Transmission Method](#) to share Information with one another. [SEEMail is designed to facilitate](#)

~~the secure exchange of email and attachments between participating agencies in a manner that protects the information against disclosure to anyone outside of the SEEMail environment.~~

~~If Information is shared by IR via SEEMail, it will be received by NZ Police a Participating Agency in a designated secure email inbox. Once received, it (rather than the individuals to whom it relates) will be given a unique identifier (for the purposes of file management) and held by NZ Police the Participating Agency in a secure registry on a secure floor. Specific security access is required to access that registry and floor environment.~~

~~IR may also, in addition to using SEEMail, share Information with NZ Police a Participating Agency by other means, for example, by permitting NZ Police that Participating Agency to physically access IR premises to examine and copy and/or remove the Information, e.g., a hard drive, computer file, hard copy files etc.~~

Information will only be distributed within NZ Police a Participating Agency to Appropriately Authorised Staff, for the purposes set out in this Agreement. Information will be distributed with specific caveats and rules to ensure the Information remains protected.

11. Safeguards to protect privacy and security

Test for sharing Information

Before any Information is requested or released, the relevant test in clause 4 must be satisfied. As noted above, senior personnel within each agency Party will be responsible for the relevant decision-making by their agency that Party. In addition, Information will only be accessible by those Appropriately Authorised Staff who need to use it for the purposes of this Agreement and who have signed certificates of confidentiality under the TAA.

Secure sharing of Information

As noted above, ~~SEEMail a Secure Transmission Method~~ will ~~primarily~~ be used to share Information between ~~IR and NZ Police the Parties~~. ~~Both agencies The Parties must~~ have information technology systems that comply with the applicable government security levels.

If SEEMail is used ~~appropriately~~ by ~~participating agencies the Parties~~, users can be highly confident that:

- Email marked [SEEMAIL] can only be read by someone on the SEEMAIL network the participating agency of the recipient, either IR or NZ Police.
- The email does in fact come from the participating agency as Party claimed.
- No one outside the sender's participating agency sending Party can read the email when it is in transit.
- No one outside the sender's participating agency sending Party can alter the message.
- Email marked [SEEMAIL] cannot be inadvertently sent to a party that is not on the SEEMAIL network non-participating agencies.
- All email traffic between participating agencies Parties is secured.
- All email traffic between participating agencies Parties authenticates the sending agency Party.

~~The Parties are investigating greater use of MFT to transfer Information between them. As part of this, they will explore using and may in the future use MFT to transfer Information under this Agreement rather than SEEMail.~~

Reasonable and practicable steps will be taken by the Parties to maintain security during any physical access, examination, copying and removal of Information. For example, where practicable physical media devices ([Ironkeys](#)) will be encrypted and password protected before removal from IR. Onsite access by [NZ Police Participating Agency](#) will also be closely supervised by IR to ensure that only Information able to be shared under this Agreement is accessed, examined, copied and removed.

Verification of Information/confirmation of identity

When [NZ Police Participating Agency](#) requests Information about one or more identifiable Individuals, IR will compare the details about the Individual(s) provided by the [NZ Police Participating Agency](#) with the details IR holds so as to have a high degree of confidence that the correct Information is shared.

Where [NZ Police Participating Agency](#) requests Information about an identifiable Individual's family members, for example, without providing identifying details of who they are, IR may need to rely on its own information.

[NZ Police Participating Agency](#) will use standard investigative processes to independently verify that Information received from IR is accurate. The process of further investigation or development of the Information will be aimed at verifying the circumstances and accuracy of the Information through corroboration with information from other sources.

Disclosure

[NZ Police and IRA Participating Agency](#) will not provide Information obtained [from IR](#) under this Agreement to ~~other another agencies Participating Agency~~ or any other third party, except as required by law or the courts. For example if Information shared under this Agreement is used by [NZ Police Participating Agency](#) as part of a criminal prosecution it may be required to be disclosed under the Criminal Disclosure Act 2008. Nothing in this Agreement limits the requirements of that Act.

Storage of Information

~~[NZ Police and IRA Participating Agency](#) will receive and store Information received under this Agreement [securely and separately from other information that it holds. via SEEMail in a designated secure email inbox. The information in this email inbox will be segregated from other information that NZ Police and IR hold. Information received in physical form will be stored according to NZ Police protocols and will similarly be kept segregated from other information that NZ Police hold.](#)~~

Transfer of Information within [NZ Police Participating Agency](#)

The Information will only be distributed to Appropriately Authorised Staff, for the purposes set out in this Agreement. [NZ Police Participating Agency](#) will not make such Information generally available to all [NZ Police of its](#) employees or anyone ~~engaged by NZ Police that it engages~~.

The Information will be distributed to Appropriately Authorised Staff in a manner which ensures that the Information is kept separate from all other information while it is being transferred and is not at risk of being mixed or overheard (as applicable). The Information will be tagged with specific rules and caveats on how the Information may be used to ensure that the Information is not used inappropriately and remains protected.

IR Training

The authorised staff of IR will be appropriately trained and/or issued with guidelines to ensure that the test is met before Information is shared under this Agreement.

Retention and deletion of Information

Relevant information

~~NZ Police~~ A Participating Agency will make an initial decision as to whether Information shared by IR under this Agreement is required for any of the purposes set out in this Agreement, within 90 days of receipt of that Information. If ~~NZ Police~~ A Participating Agency decides that it no longer requires the Information, it will inform IR of that decision within 14 days of making the decision.

Information that is shared and held by ~~NZ Police~~ A Participating Agency that is required for any of the purposes set out in this Agreement will be retained by ~~NZ Police~~ that Participating Agency for as long as required and in accordance with the Public Records Act 2005 and any applicable disposal authorities under that Act. Given that matters concerning Serious Crimes are usually complex, this retention period may extend over a number of years, both for active cases and in situations involving cold cases. ~~Destruction thereafter is subject to the requirements of the Public Records Act 2005 and any applicable disposal authorities under that Act.~~

Information that is not relevant or no longer required

Information shared with ~~NZ Police~~ A Participating Agency ~~by SEEMail~~ that is not relevant or no longer required by ~~NZ Police~~ that Participating Agency for the purposes set out in this Agreement will be deleted from operational files within 90 days of the non-requirement decision being made (such decision being required within 90 days of receipt of the Information), subject to the requirements of the Public Records Act 2005 and in accordance with any applicable disposal authorities under that Act. (Information in physical form that is not required by ~~NZ Police~~ A Participating Agency will also be destroyed, or returned to IR at IR's request, within 90 days of the non-requirement decision, subject to the requirements of the Public Records Act 2005 and in accordance with any applicable disposal authorities under that Act.)

~~IR records of Information requests from NZ Police and the responses to those requests, and IR records of the proactive provision of Information to NZ Police, will be deleted from operational files within 90 days of receipt of a non-requirement decision from NZ Police, subject to the requirements of the Public Records Act 2005 and in accordance with any applicable disposal authorities under that Act. IR Participating Agencies may retain administrative records documenting the fact that requests were received-made and transfers occurred in accordance with the Public Records Act 2005.~~

The ~~NZ Police Participating Agency~~ deletion/destruction/return obligation applies to Information shared by IR only and not to Information that a Participating Agency has obtained independently ~~by NZ Police. The IR deletion obligation applies to records of Information requests and responses, and to the records of proactive releases of Information to NZ Police, but not to the original collections of Information held by IR.~~

IR Retention

~~If IR does not receive a non-requirement decision following the initial provision of Information to NZ Police (as outlined above) IR will retain its records of Information requests and of the nature and amount provision of Information provided and its associated decision-making processes (including any subsequent non-requirement decisions) in accordance with its retention and disposal schedule under for a period of 7 years following which the records will be deleted, subject to the requirements of the Public Records Act 2005, and any applicable disposal authorities under that Act. IR may retain administrative records documenting the fact that requests were received and transfers occurred in accordance with the Public Records Act 2005.~~

Codes of conduct

All staff at IR must follow the IR's code of conduct, which prohibits the disclosure of any information obtained from their work unless they have authority to do so. IR officers must also comply with the secrecy confidentiality obligations in section ~~8+18~~ of the TAA which provides that all such officers must keep confidential all sensitive revenue information secret matters relating to the Inland Revenue Acts (except to the extent that an exception in the TAA applies disclosure is permitted under the TAA). IR contractors must comply with similar obligations.

~~NZ Police~~Participating Agency employees and anyone engaged by ~~NZ Police~~a Participating Agency must comply with the ~~NZ Police~~Participating Agency's Code of Conduct (if any), its policies relating to integrity and confidentiality, the State Services Commission Code of Conduct, and other applicable policies and legislative obligations. The Police Code of Conduct, for example, prohibits unauthorised access to, or disclosure of, any matter or information in relation to Police business.

~~NZ Police~~Participating Agency employees may on occasion find themselves privy to information that, although it is legitimately obtained for ~~NZ Police~~Participating Agency business purposes, may set up a conflict of interest, or create tension between ~~NZ Police~~Participating Agency duties and personal obligations. ~~NZ Police~~Participating Agency employees, and others with authorised access to ~~NZ Police~~Participating Agency information, must declare such personal or private interest in official matters to management and accept and abide by decisions that they should have no further involvement in the matter, and not receive or seek out any further information about it.

Privacy ~~breaches~~ incidents

Where Personal Information ~~is found to~~may have been inappropriately accessed, used or disclosed, ~~IR's and NZ Police's~~the relevant Parties' internal investigation processes will be applied.

Where an internal investigation confirms the loss or potential loss of, or unauthorised access to, Personal Information, amounting to a material-notifiable privacy breach, the Privacy Commissioner will be notified as soon as possible/practicable.

Where an internal investigation is undertaken, the Party undertaking the investigation will liaise with the appropriate personnel at other agencies if applicable.

Audit

The Parties will undertake an audit of the operation of this Agreement on an annual basis to check that the safeguards in the Agreement are operating as intended, that they remain sufficient to protect the privacy of individuals and to ascertain whether any issues have arisen in practice that need to be resolved.

12. Assistance statement

~~IR and NZ Police~~The relevant Parties will provide any reasonable assistance that is necessary in the circumstances to allow the Privacy Commissioner or an individual who wishes to make a complaint about an interference with privacy to determine the agency-Party against which the complaint should be made.

If a Participating Agency receives a request from an individual for information about this Agreement, or for their Personal Information exchanged under this Agreement, the Participating Agency will consult with IR before releasing the information.

13. Security and privacy provisions

If ~~either a~~ Party has reasonable cause to believe that any breach of any security or privacy provisions in or referred to in this Agreement has occurred or may occur, that Party may undertake investigations in relation to that actual or suspected breach as deemed necessary. ~~Both~~ Parties shall ensure that reasonable assistance is provided to the investigating Party in connection with all inspections and investigations. The investigating Party will ensure that the ~~other~~relevant party is kept informed of any developments. Compliance by IR officers with this obligation is subject to their obligations under the TAA.

~~Either A~~ Party may suspend its participation in this Agreement to allow time for a security breach to be remedied.

14. Dispute resolution

Should any dispute or differences relating to the interpretation or application of this Agreement arise; the relevant Parties will meet in good faith with a view to resolving the dispute or difference as quickly as possible.

If the relevant Parties are unable to resolve any dispute within 60 days, the matter shall be referred to their Commissioner/Director/Comptroller (as applicable) ~~CNZP and the CIR~~, or their delegated representatives, for resolution.

The relevant Parties shall continue to comply with their obligations under this Agreement despite the existence of any dispute.

15. Review of the Agreement

A joint review of the Agreement may be undertaken whenever ~~either a~~ Party believes that such a review is necessary.

The lead agency shall conduct a review annually or at intervals specified by the Privacy Commissioner. The report will be included in the agency's annual report.

The Parties shall co-operate with each other in any review and will take all reasonable actions to make the required resources available.

16. Amendments to the Agreement

Any amendments to this Agreement must be in writing and signed by the Commissioners of IR and NZ Police, the Director of SFO and the Comptroller of NZ Customs ~~CNZP and the CIR~~, or their delegates.

Amendments to the Agreement will be made in accordance with section 96V of the Privacy Act 1993.

Should the Parties be unable to agree on amendments to the Agreement the matter shall be dealt with in accordance with clause 14 above.

17. Term, performance and termination

This Agreement comes into force on the date that it is signed by ~~both~~ all of the Parties.

The Agreement shall continue in force until ~~either the CNZP or the CIR terminates the Agreement~~ all of the Parties agree to terminate it, or the Order in Council is revoked.

~~Either A~~ Party may suspend, limit, or terminate its participation in this Agreement if it appears to that Party that the terms of the Agreement or the Order in Council are not being met or the Information sharing under this Agreement is otherwise unlawful.

The obligations in the Agreement which concern confidential information and secrecy shall remain in force notwithstanding the termination of the Agreement.

If extraordinary circumstances arise (including but not limited to earthquake, eruption, fire, flood, storm or war) which prevent ~~either a~~ Party from performing its obligations under the Agreement, the

performance of that Party's obligations shall be suspended for as long as those extraordinary circumstances prevail.

18. Departmental representatives

Each Party will appoint a contact person to co-ordinate the operation of this Agreement with the other Party and will ensure that the contact person is familiar with the requirements of the Privacy Act 1993, the Information sharing initiative and this Agreement. The initial contact persons are as follows:

Inland Revenue

[Manager Investigations Group Lead,
Customer Compliance](#)

[New Zealand Customs Service](#)

[Manager: Intelligence](#)

New Zealand Police

[Manager, National Manager
Intelligence Centre](#)

[Serious Fraud Office](#)

[General Counsel](#)

All notices and other communication between the Parties under the Agreement shall be sent to the contact persons specified above.

The contact person set out above may be updated from time to time by notice (which may be by email) to the other ~~Party~~Parties. ~~Both The~~ Parties are to ensure that the Privacy Commissioner is informed of the current contact persons for this Agreement if they are not those set out above.

Information Sharing Agreement

Between

Inland Revenue

And

**New Zealand Police, New Zealand Customs Service and
Serious Fraud Office**

Relating to

**Disclosure of information by Inland Revenue for the purpose of prevention,
detection, investigation or providing evidence of serious crime**

**Pursuant to Part 9A of the Privacy Act 1993 and section 18E(2) of the Tax
Administration Act 1994**

August 2019

Contents

Defined terms 4

Background 6

Terms 6

1. Objectives and purpose of the Agreement 6

2. Exemptions and/or modifications to information privacy principles 7

3. The public service or public services the provision of which the Agreement is intended to facilitate 7

4. Type of Information to be shared under the Agreement 7

5. The Parties involved and the lead agency 7

6. Description of Information to be shared between IR and each Participating Agency 8

7. How the Parties may use the Information 8

8. Adverse actions 9

9. Where you can view this document 10

10. Overview of the operational details 16

11. Safeguards to protect privacy and security 17

12. Assistance statement 20

13. Security provisions 20

14. Dispute resolution 21

15. Review of the Agreement 21

16. Amendments to the Agreement 21

17. Term, performance and termination 21

18. Departmental representatives 22

Information Sharing Agreement

[Insert clean copy]

DRAFT

20 August 2019

Naomi Ferguson
Commissioner of Inland Revenue
Inland Revenue
PO Box 2198
Wellington 6140

Dear Naomi,

Privacy Commissioner's submission on the proposed extension to the information sharing agreement with the New Zealand Police to prevent, detect, investigate or provide evidence of serious crime

This submission is provided under section 96O of the Privacy Act 1993 regarding the proposed extension of the approved information sharing agreement ("AISA") with the New Zealand Police to include the New Zealand Customs Service (Customs) and the Serious Fraud Office (SFO) as parties. Following changes to the proposed extended AISA, this replaces my submission of 28 November 2018. The purpose of the AISA remains the same: to support the goal of reducing the rate of serious criminal offending in New Zealand.

For Customs and SFO, the extension of the AISA will assist those agencies to identify, investigate and prosecute serious crime, including fraud and corruption.

The principal reason an AISA is required is to permit Inland Revenue (IR) to share information where that sharing would otherwise breach tax secrecy provisions. Under the Privacy Act, collection and disclosure of personal information is permitted where that is necessary for public sector agencies to avoid prejudice to the maintenance of the law, including the detection, prevention, and investigation of offences, subject to any relevant limitations under other enactments, including section 21 of the New Zealand Bill of Rights Act 1990.

Overall, I am satisfied that the AISA meets the requirements set out in Part 9A of the Privacy Act, in particular those set out in section 96N.

My comments are set out below, referring to the criteria in section 96N of the Privacy Act. I intend to publish these comments following the making of the Order in Council.

These comments are without prejudice to my position on what will constitute appropriate monitoring of compliance with this agreement, under the provisions of sections 96S-96U of the Privacy Act.

1. Does the information sharing agreement facilitate the provision of any public service or public services?

The information sharing agreement between IR, NZ Police, SFO and Customs will assist those agencies to deliver the public service of maintaining public safety, law enforcement and crime prevention. In particular the prevention, detection, and investigation of serious crime and the provision of evidence of serious crime.

Sharing under the amended agreement can either be because of:

- a request by NZ Police, SFO or Customs (defined in the AISA as 'Participating Agencies') to IR, or
- through IR proactively sharing information with a Participating Agency where it has reasonable grounds to suspect that the personal information meets the threshold for sharing under the agreement. The threshold for serious crime remains set at an offence which is punishable by at least four years imprisonment.

2. Is the type and quantity of personal information to be shared under the agreement no more than is necessary to facilitate the provision of that public service or those public services?

The types of information that may potentially be shared are broad, as set out in clause 3 of the agreement. The types include information about an individual's associates, tax information, financial transaction information, financial relationship information, domestic relationship information, information about assets, employment information, person records and social assistance information. IR may also proactively share any other type of information, with the exception that it may not share information obtained under sections 17I or 17J of the Tax Administration Act with the NZ Police or Customs.

I consider that the type and quantity of personal information to be disclosed by IR to the Participating Agencies is appropriate for the purposes of prevention, detection, investigation or providing evidence of a serious crime.

The extension of the AISA to include Customs and SFO increases the amount of information shared, and consequently the risk of a privacy breach is heightened. The information shared about each individual, and potentially their domestic or financial partners, is sensitive and wide-ranging and needs to be well protected.

The flow of information under this agreement is predominantly from IR to a Participating Agency on request. However, for reactive sharing situations IR will receive personal information from a Participating Agency to enable it to identify an individual in its records and assess whether information can be provided under the agreement.

3. Will the agreement unreasonably impinge on the privacy of individuals and contain adequate safeguards to protect their privacy?

Information sharing under the agreement may result in significant adverse actions such as investigation, arrest and prosecution being taken by a Participating Agency. Information

provided by IR under this AISA is not only about suspected criminal offenders but in some instances may be information about the victim of a serious offence. If a victim's details were to be compromised because of sharing under this agreement, the intrusion on their privacy could be significant.

Except to the extent that IR's locating and sharing of personal information with a Participating Agency could be considered an adverse action, the AISA states that IR will not take adverse action under this agreement.

Under section 14(a) of the Privacy Act I must have due regard to the protection of social interests that compete with privacy. I am satisfied that the agreement contains adequate safeguards to protect the privacy of individuals and not to unreasonably impinge of their privacy. These safeguards are outlined in the Appendix to this letter.

I consider the risk mitigating steps detailed in the AISA are appropriate safeguards to limit the impact on privacy in the circumstances. The AISA provides specific checks and assurances about handling personal information that ensure the information sharing is proportionate and justified in the circumstances and does not unreasonably impinge on people's privacy.

4. Will the benefits of sharing personal information under the agreement be likely to outweigh the financial and other costs of sharing it?

Inland Revenue reported the estimated cost of the sharing agreement with NZ Police as \$9,500 for the 2017/18 period. When asked about estimated costs, IR officials advised that it did not have an estimate of the costs associated with the extension of the AISA but based on the current sharing with the NZ Police, costs are also estimated to be low.

The forecast volume of additional sharing under the agreement is relatively small, with an estimated 20 shares with SFO and 200+ shares with Customs annually.

Of the 222 times that IR shared information with NZ Police during 2017/18, there were 70 instances where information was used in a case with a resolution of prosecution. Based on these results, I accept that the extension of the agreement will assist SFO and Customs in detecting, investigating and prosecuting serious crime.

5. Are there any potential conflicts or inconsistencies between the sharing of personal information under the agreement and any other enactment, and have they been appropriately addressed?

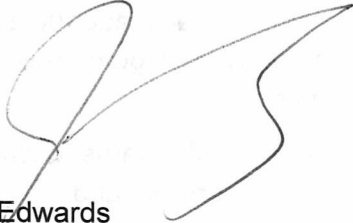
I am not aware of any potential conflicts or inconsistencies that will impact on this proposal. While IR is generally required to keep sensitive revenue information confidential in accordance with section 18 of the Tax Administration Act, section 18E(2) of that Act provides this does not apply to disclosures in accordance with an agreement approved by Order in Council made under Part 9A of the Privacy Act.

I note that the agreement does not cover information sharing as part of the Criminal Proceeds (Recovery) Act 2009. Nor does the agreement purport to override any provisions

in any enactment other than the Privacy Act 1993 as authorised by Part 9A. The Participating Agencies must comply with all relevant provisions of their own legislation and the agreement does not authorise information sharing that would be inconsistent with section 21 of the New Zealand Bill of Rights Act 1990.

I hope that these comments are helpful in finalising approval of the Agreement by Order in Council.

Yours sincerely

A handwritten signature in black ink, appearing to read 'John Edwards', written over a faint, illegible stamp.

John Edwards
Privacy Commissioner

Appendix: Safeguards in the AISA to protect the privacy of individuals

- The parties to the agreement are required to have sufficiently robust controls in place to ensure information is appropriately managed, including:
 - limiting decision making responsibilities to senior staff
 - secure electronic communication of information
 - identity and information verification protocols
 - information distributed with specific caveats and rules, and
 - protocols for data retention and destruction.
- The sharing is targeted to cases the parties consider will assist in the prevention, detection or investigation of suspected serious criminal offending and is limited to information that is relevant to such offending.
- When requesting information from IR, a Participating Agency must confirm it reasonably believes that the amount of Information it has requested is reasonable and proportionate in the circumstances, and have taken all reasonable steps to obtain the information from other available sources without success (where practicable).
- The test for sharing requires IR to verify that it is reasonable, proportionate, practicable and in the public interest to provide the Information to the Participating Agency, whether sharing that information as a response to a request or proactively.
- IR may not share with the NZ Police and Customs any information it has obtained by compulsion using its powers under sections 17I and 17J of the Tax Administration Act.
- IR may only share information obtained under sections 17I and 17J of the Tax Administration Act with the SFO on request where the SFO confirms there are reasonable grounds to believe that an offence involving serious or complex fraud may have been committed, in addition to meeting the relevant test for sharing as set out in clause 4 of the agreement.
- Information obtained under sections 17I and 17J of the Tax Administration Act that is shared with the SFO on request is subject to the limitation in section 17K of the Tax Administration Act (statements made by a person in answer to a question put to them in the context of an inquiry is not admissible in criminal proceedings except on a charge of perjury).
- The information shared will only be used by a Participating Agency for the purposes of the agreement (the prevention, detection, investigation or prosecution of a Serious Crime) and cannot be used as evidence of a non-Serious Crime, for data analytics, as general intelligence information, or for vetting purposes.
- Any adverse action in the form of a prosecution is subject to the Solicitor General's Prosecution Guidelines, and is subject to the disclosure requirements of the Criminal Disclosure Act 2008.
- Information shared under the agreement will not be disclosed to other Participating Agencies or any third party, except as required by law.
- Information shared that is not relevant or is no longer required must be deleted, as set out in clause 11 of the agreement.
- The parties are required to undertake an annual audit of the operation of the agreement to check the safeguards in the agreement are operating as intended, remain sufficient to protect the privacy of individuals and to ascertain if any issues have arisen in practice that need to be resolved.

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 crime¹ 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

¹Serious 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 opinion² 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,³ and therefore has not been included in the original or the proposed information sharing.

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

³ 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 proposals⁴ 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.

⁴ <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>)	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 (<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
Total Monetised Cost		Low
Non-monetised costs		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
Total Monetised Benefit		Unable to estimate
Non-monetised benefits		<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.⁵

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

⁵ThinkPlace, *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.



Cabinet Social Wellbeing Committee

Minute of Decision

This document contains information for the New Zealand Cabinet. It must be treated in confidence and handled in accordance with any security classification, or other endorsement. The information can only be released, including under the Official Information Act 1982, by persons with the appropriate authority.

Extending the Serious Crime Information Sharing Agreement

Portfolio **Police / Revenue / Customs**

On 18 September 2019, the Cabinet Social Wellbeing Committee:

- 1 **noted** that information sharing concerning taxpayer information may take place under Part 9A of the Privacy Act 1993 through an Order in Council using the Approved Information Sharing Agreement (AISA) mechanism;
- 2 **noted** that in September 2018, the Cabinet Social Wellbeing Committee agreed to release the draft Information Sharing Agreement, and associated discussion document, between Inland Revenue, the New Zealand Police, the New Zealand Customs Service, and the Serious Fraud Office, for public consultation [SWC-18-MIN-0128];
- 3 **agreed** to the preparation of the extension of the Serious Crime AISA to enable the sharing of information from Inland Revenue to the Serious Fraud Office, and to Customs;
- 4 **authorised** the Minister of Revenue and Minister Responsible for the Serious Fraud Office, in conjunction with the Minister of Customs where appropriate, to make decisions on the detailed implementation of these proposals, in line with the decisions taken in the paper under SWC-19-SUB-0128;
- 5 **invited** the Minister of Revenue to instruct the Parliamentary Counsel Office to prepare draft Orders in Council, which will approve the information-sharing agreement, in accordance with the Privacy Act 1993, as well as consequential Order to repeal the existing sharing provision between Inland Revenue and the Serious Fraud Office.

Vivien Meek
Committee Secretary

Hard-copy distribution (see over)

Present:

Rt Hon Winston Peters
Hon Kelvin Davis
Hon Grant Robertson
Hon Chris Hipkins
Hon Andrew Little
Hon Carmel Sepuloni (Chair)
Hon Tracey Martin
Hon Willie Jackson
Hon Poto Williams
Jan Logie, MP

Officials present from:

Office of the Prime Minister
Officials Committee for SWC
Office of the SWC Chair

Hard-copy distribution:

Minister of Police
Minister of Customs