

Regulatory Impact Statement: Information sharing between Customs and supply chain participants for border security purposes

Decision sought	Analysis produced for the purpose of informing Cabinet decisions on proposals to amend the Customs and Excise Act 2018
Agency responsible	New Zealand Customs Service
Proposing Ministers	Minister of Customs
Date finalised	10 July 2025

The Regulatory Proposal

The regulatory proposal is to provide within the Customs and Excise Act 2018 (CEA) for agreements to be entered into by the chief executive of Customs with supply chain participants¹ to facilitate the two-way sharing of information between the parties to the agreement covering:

- specified supply chain integrity information such as information provided by Customs to the supply chain participant of interceptions of illicit commodities, and information from supply chain participants to Customs concerning breaches of security systems
- specified personal information from Customs to a Customs-controlled area (CCA)² or other New Zealand based supply chain participant where Customs reasonably believes there is heightened border security risk posed by employees of, and those with access to, CCAs or other New Zealand based supply chain participants' facilities and operating systems.

Summary: Problem definition and options

What is the policy problem or opportunity?

Supply chain participants (SCP) and Customs need to work together to strengthen supply chains against transnational, and serious organised crime (TSOC), and insider threats especially. Two-way information sharing is central to achieving this objective. There is no clear established means to create an ongoing commitment to the sharing of border security information, which gives comfort to SCP (particularly those that might be sharing information sourced or held overseas) that information sharing by them is supported legally and will not result in adverse or prejudicial outcomes for them.

¹ A supply chain participant is any entity with legitimate interest in the secure, lawful transboundary movement of goods. It includes, but is not limited to operators of a CCA, freight forwarders, Customs brokers, airlines, shipping operators, stevedore and marine cargo handling suppliers with CCA access, other third parties operating in or with access to a CCA.

² A CCA is licensed by Customs as a secure and controlled environment that is approved to conduct certain functions or activities such as processing international passengers and loading or unloading cargo and items.

Globally, supply chain vulnerabilities are increasingly being exploited by TSOC groups. This is being exacerbated through the increasing use by TSOC groups of trusted insiders³ to circumvent border controls.

Information from SCP concerning breaches of their security systems would support improvements to Customs' border risk assessment and targeting activities, and information from Customs to SCP on interceptions of illicit commodities would assist SCP to identify and address vulnerabilities in their security systems and supply chains. Information sharing needs to be done in a way that does not jeopardise ongoing investigations.

There are hundreds of SCP which vary considerably in scale and scope, and therefore in their border security risk profile. At one end of the scale are entities such as ports and airports, and multinational shipping and freight companies. At the other end are smaller or specialised entities. The systematic and ongoing sharing of information for border security purposes would achieve the most benefit in relation to larger and more diverse SCP, and in particular those that operate internationally. The problem is how to overcome the barriers to information sharing taking place, and to ensure that appropriate protections and restrictions are transparently applied when the sharing of personal information is involved. The principal presenting problems and issues are:

- how to establish an ongoing commitment to the sharing of information
- giving comfort to SCP (particularly those that might be sharing information sourced or held overseas) that information sharing by them is both legal and necessary and will not result in adverse or prejudicial outcomes for them
- agreeing and enforcing limitations on how any information shared may be used, and acceptable standards for its storage, on-sharing, and disposal
- providing transparency where personal information may be shared and under what conditions, and how that relates to the information privacy principles established in the Privacy Act 2020.

The information disclosure regime contained in section 317 of the CEA which can be used for ongoing information disclosure by Customs to private sector organisations is not suitable to apply to the particular circumstances needed to work with SCP to improve supply chain security and combat TSOC. This is because agreements made under section 317:

- cannot operate on a two-way basis ie Customs to SCP and SCP to Customs
- cannot be made with an overseas based private sector organisation.

Because of the above limitations the exceptions available under the Privacy Act are applied when personal information is included in information to be shared with SCP. Where the link between the disclosure and a clear law enforcement purpose is less obvious (for example, Customs providing interception information that may contain some personal information to SCP so that they can identify and address potential vulnerabilities in their supply chain) Customs is more likely to take a conservative approach in determining whether to disclose information, to avoid a potential privacy breach and the subsequent risk of reputational damage. The reluctance to disclose where the limits of disclosure are unclear means that opportunities to detect or prevent offending may be missed.

³ A trusted insider is any person who, through their employment (past or present) in a supply chain business, uses their access to goods, systems or premises for malicious purposes.

What is the policy objective?

The objective is to improve border security through the transparent, efficient, and proportionate sharing of border security risk information between Customs and SCP, while ensuring the principles in the Privacy Act 2020 are applied to any personal information that is shared.

What will success look like?

Success would be indicated by the willingness of key SCP to enter into an information sharing agreement with Customs, noting that entering into an agreement will be voluntary and therefore each party will have the opportunity to assess the relative costs, benefits and impacts part of that decision process. Given the feedback from industry during targeted engagement, it is considered that SCPs are willing to participate in the interests of improving the resilience of their systems and contributing to improved border security.

Noting that information sharing is not an end in itself, wider success in terms of achieving government objectives to combat TSOC would be indicated by the usefulness of the information shared in initiating follow up actions to improve Customs' border risk assessment and targeting activities and/or for SCPs to address vulnerabilities in their security systems and supply chains.

Options considered

Option one - status quo – facilitating systematic and ongoing sharing of supply chain security related information between Customs and SCP through the existing information disclosure regime in the CEA (which permits, through written agreements, Customs to disclose information to private sector organisations where the information would be required to be made available under the Official Information Act 1982), and through applying the Privacy Act 2020 when personal information is to be shared.

Option two - amend the CEA to clarify and enable two-way border security information sharing (preferred option).

Option two is preferred. This option would build off the approach contained in the CEA for information disclosure by Customs to private sector organisations based on written agreements that are voluntarily entered into by the two parties at the chief executive level.

Option two is preferred over option one as it creates a regulatory framework to address the barriers and issues with regular ongoing two-way sharing of information for border security purposes and which facilitates Customs and SCP working together to deliver on the wider objective of more effective border security. Option two gives a means to establish an ongoing commitment to the sharing of information and will give comfort to SCP (particularly those that might be sharing information sourced or held overseas) that information sharing by them is supported legally and will not result in adverse or prejudicial outcomes for them.

Under option two the essential features already required in the information sharing regime in the CEA would apply covering such matters as specifying the process for making an agreement, the type of information that can be shared, the purposes for which it can be shared, the purposes for which it can be used and retained, and other relevant details (such as requirements relating to on-sharing, storage and disposal). Information shared under an agreement may not be used for a prejudicial purpose, such as for evidential purposes or in disciplinary proceedings against an employee, without the prior written approval of the party that supplied the information.

Option two promotes efficiency in information sharing through clear specification in a written agreement of the scope of information shared and the conditions for sharing it thus

simplifying decision-making and supporting a consistent approach to the application of caveats and conditions.

Option two gives transparency over any personal information being shared as it would include features already required in the information sharing regime in the CEA to require agreements to clearly specify limitations on how any personal information shared may be used, and the minimum acceptable standards for its storage, on-sharing, and disposal. Option two is assessed as providing a reasonable balance between an individual's right to privacy and achieving the broader societal benefits from improved border security.

What consultation has been undertaken?

Customs has undertaken targeted engagement with SCP (including ports, airports, freight forwarders, and logistics companies). These stakeholders all indicated an awareness of and concern about the problems in information sharing for border security purposes and were supportive of an information sharing framework being established in the CEA.

Customs will continue to engage with industry stakeholders as legislation is developed and implemented. Customs is engaging with the Office of the Privacy Commissioner.

Consultation was undertaken with the following agencies; Department of Prime Minister and Cabinet, Ministry of Justice, Ministry of Business Innovation and Employment (New Zealand Immigration Service), New Zealand Security Intelligence Service, Government Communications Security Bureau, New Zealand Police, Ministry for Primary Industries, Ministry of Defence, and Te Puni Kōkiri.

Is the preferred option in the Cabinet paper the same as preferred option in the RIS?

Yes.

Summary: Minister's preferred option in the Cabinet paper

Costs

The monetised costs are estimated to be low with a high level of certainty. The costs are:

- one-off costs for Customs to make legislation, and update operational policies and procedures
- ongoing costs for Customs to maintain policies and procedures, and provide training
- upfront and ongoing costs to Customs and an individual SCP associated with putting in place and maintaining an information sharing agreement. Entering into an information sharing agreement will be voluntary and therefore each party will have the opportunity to assess the relative costs, benefits and impacts of an agreement as part of that decision process.

The preferred option is expected with a high degree of certainty to not increase Customs' day to day operational costs. To ensure that these agreements are not overly bureaucratic, time consuming and costly to develop, Custom proposes to develop a template agreement in consultation with the Office of the Privacy Commissioner.

There are expected to be minimal costs to SCP in sharing the information covered by an agreement. There may be some costs involved in the collation and provision of information, although these will be minimal as the information that will be included in an agreement is that which would ordinarily be held by a business in a readily retrievable manner.

Customs and SCP may face costs associated with justifying any information held and shared in the event of a complaint (for example, the resources spent responding to a complaint made to the Office of the Privacy Commissioner or some other relevant body, if an individual considers their privacy has been breached). This will be managed through controls and processes already established within the parties to an agreement to ensure compliance with the Privacy Act and to act on complaints, and through information sharing arrangements specifying controls on personal information in a clear and transparent way.

Benefits

The scale of benefits cannot be quantitatively measured and therefore have to be qualitatively assessed against the costs and impacts.

There is confidence that the proposal will achieve net benefits by facilitating and supporting two-way information sharing to generate improvements to Customs' border risk assessment and targeting activities and to assist SCP to identify and address vulnerabilities in their security systems and supply chains. It is expected the preferred option will contribute to both improved resilience of supply chains to TSOC activity and improved detection of and disruption to TSOC activities. It may have the indirect benefit of also assisting SCP to improve the safety of workplaces.

These outcomes will also contribute to New Zealand maintaining its international reputation as a relatively corruption free and low risk trading partner.

Balance of benefits and costs

The benefits of the preferred option are likely to outweigh the costs.

The initial and ongoing costs in changing legislation and updating policies and procedures will be low. The costs to Customs and an individual SCP associated with putting in place and maintaining an information sharing agreement are expected to be low, noting that entering into an information sharing agreement will be voluntary and therefore each party will have the opportunity to assess the relative costs, benefits and impacts of an agreement as part of that decision process.

The scale of the actual costs and harms being imposed on society by TSOC groups are high and so even a marginal increase in the deterrence, detection and combatting of TSOC activity through information sharing will be beneficial if it can be achieved at low cost.

Implementation

Changes to the CEA are required for implementation, which will be led by Customs. Royal Assent of the Customs and Excise (Border Security) Amendment Bill is expected by late 2026.

Implementation will require information sharing agreements to be in place between Customs and SCP. To ensure these can be developed and implemented in a timely manner a template will be developed in consultation with the Office of the Privacy Commissioner.

Limitations and Constraints on Analysis

The analysis is based on the assumptions that:

- TSOC-related threats will continue and increase over time if unchecked
- clear and enabling legislation in respect of border security information sharing will support actions by Customs and SCP to improve border and supply chain security.

A limitation of this analysis is that the costs and benefits can only be analysed qualitatively due to an absence of hard data. Information sharing is not an end in itself and the impact of an individual information sharing agreement on the wider objectives in relation to TSOC depends on the usefulness of the information shared and resulting follow up actions.

I have read the Regulatory Impact Statement and I am satisfied that, given the available evidence, it represents a reasonable view of the likely costs, benefits and impact of the preferred option.

Responsible Manager(s) signature:

S9(2)(a)

Group Manager Policy and Strategy
10 July 2025

Quality Assurance Statement	
Reviewing Agency: New Zealand Customs Service	QA rating: Meets
Panel Comment: The New Zealand Customs Service Regulatory Impact Analysis Panel has reviewed the Regulatory Impact Statement and considers the information and analysis summarised in the RIS meets the Quality Assurance criteria.	

Section 1: Diagnosing the policy problem

Transnational serious and organised crime is causing significant harm

1. Transnational, serious and organised crime (TSOC) undermines New Zealand's sovereignty by breaching its borders (illicit goods), and undermining its institutions (fraud and corruption), and financial systems (money laundering). Combatting and disrupting the activities of TSOC and in particular the smuggling of illicit drugs and firearms, and its associated activities such as money laundering and immigration fraud, is a high priority national security objective.
2. The threats from TSOC groups are an ongoing border security risk for New Zealand. In the financial year 2023/24 Customs seized 4,800 kg of methamphetamine bound for NZ and detected \$10.9 million in undeclared cash at the border. There is evidence that TSOC is expanding globally, taking advantage of improved technology for nefarious purposes, global instabilities to exploit weak governance, and the lure of high financial returns.
3. In New Zealand, intercepts of methamphetamine at the border have doubled in the period 2018 – 2024, while the weight of those intercepts has increased 14-fold. Also, waste-water testing indicates usage has doubled in the past calendar year alone which is evidence that comparatively high volumes of imported illicit substances are reaching the domestic market undetected.
4. TSOC groups have developed a good understanding of border processes and procedures and the operation of international supply chains. Consequently, they exploit vulnerabilities including by corrupting and intimidating people in positions within legitimate supply chains (trusted insiders).
5. The World Customs Organisation estimates 70 percent of global maritime seizures in the past two years has had a link to a trusted insider threat. Domestically, Auckland International Airport estimates 50 percent of illicit drug seizures connected to trade and travel through the airport have a link to a trusted insider threat.
6. There have been several identified significant systemic supply chain breaches involving trusted insiders. These operations identified trusted insiders within CCAs and the supply chain (including employees who unload cargo, managers, and customs brokers⁴) who were involved in the importation of 443 kg of methamphetamine and 5 kg of MDMA.

The supply chain is comprised of various subsectors that intersect at the border

7. The global supply chain system plays a crucial role in our economy. It underpins all sectors, connecting those producing goods and materials to consumers.
8. There are several government agencies and many private sector supply chain participants (SCP) that operate across or at New Zealand's border and whose systems' security impact New Zealand's wider border security. This includes:

⁴ Customs brokers in New Zealand are trained professionals who represent importers and exporters, acting as their agent in their interactions with Customs. They prepare and lodge import and export entries onto Customs' computer system, providing mandated data in respect of the consignment.

- SCP – shipping lines, cargo owners, warehouse facilities, storage facilities, transport operators, airlines, airports, ports, manufacturers, freight-forwarders, and service providers such as stevedores and ground handlers
 - Government agencies – Customs, Immigration New Zealand, Ministry for Primary Industries, Maritime New Zealand, Civil Aviation Authority, Ministry of Health, and Ministry of Foreign Affairs and Trade.
9. The supply chain is made up of hundreds of SCP that vary considerably in scale and scope, and therefore in their border security risk profile. At one end of the scale are entities such as ports and airports, and multinational shipping and freight companies. At the other end are smaller or specialised entities. Some SCP are CCAs, for example airports, seaports, and warehouse facilities. Given their role in the supply chain, such as a place of first arrival (or final point prior to departure) CCAs are areas of heightened border security vulnerability. CCAs are particularly vulnerable to trusted insider threats.

Customs and supply chain participants need to share information to combat TSOC

10. SCP and Customs need to work together to strengthen supply chains against TSOC, and insider threats especially. Two-way information sharing is central to achieving this objective. For example, information from SCP concerning breaches of their security systems would support improvements to Customs' border risk assessment and targeting activities, and information from Customs to SCP on interceptions of illicit commodities would assist SCP to identify and address vulnerabilities in their security systems and supply chains.
11. The systematic and ongoing two-way sharing of border security information to achieve border security objectives would achieve the most benefit in relation to larger and more diverse SCPs, and in particular those that operate internationally.

Information disclosure and sharing under the Customs and Excise Act 2018

12. The disclosure and sharing of information collected by Customs in carrying out its border management functions is governed by overarching legislation (Privacy Act 2020 and Official Information Act 1982) and by a tailored information disclosure regime contained in the CEA.
13. Customs' information includes all information defined in section 304⁵ of the CEA. For the purposes of the CEA, "information" includes any information relating to persons, goods and craft, as well as intelligence assessments and reports generated by Customs. Further and specifically in relation to a person, "information" includes arrival and departure information, biometric information and passenger name record data.
14. Section 301 of the CEA requires Customs to take all reasonable steps to protect information that it collects from being unlawfully disclosed beyond Customs. That section also places restrictions on using, holding or storing personal information. Protections under

⁵ Section 304 **Category 1** information means any information held by Customs, including information relating to persons, goods, craft but excluding Category 2 information. **Category 2** information means arrival and departure information, biometric information, passenger name record information, and intelligence assessments and reports generated by Customs.

the Privacy Act 2020 also apply to personal information collected, used, held, stored or disclosed by Customs.

15. The CEA's information disclosure regime facilitates the sharing of Customs or border-related information both domestically and internationally. This includes the ability to:
 - a. disclose information to a government agency (section 316) for the purpose of assisting the government agency to carry out its functions
 - b. disclose information to private sector organisations (section 317) where the information would be required to be made available under the Official Information Act 1982
 - c. disclose information to an overseas authority (section 318) to assist the authority to carry out its functions related to or involving the protection of border security.
16. Information sharing under the CEA is through an information sharing agreement made at the Ministerial or chief executive level. These agreements are required by the CEA to cover:
 - a. the purpose of the sharing
 - b. the information to be shared
 - c. who the information is to be shared with
 - d. the legal basis for the sharing
 - e. the controls in place to ensure information is stored securely and disposed of when no longer required.
17. Agreements are designed to enable the disclosure of large data sets on an ongoing basis under limited circumstances. In general, sensitive personal or operational information held by Customs can only be shared with law enforcement agencies (domestically and internationally), and even then, only when necessary to enable that agency to carry out its functions. Further, in the case of overseas agencies, that function must be related to, or involving, the protection of border security specifically. Agreements cannot authorise another agency or organisation to provide information to Customs.
18. Information can be shared with private sector organisations (which would include SCP) under an agreement made under section 317 of the CEA. This is currently limited to information of the type that would otherwise be released under the Official Information Act 1982 (OIA). An agreement made under section 317 cannot operate on a two-way basis, or be made with an overseas based private sector organisation.
19. Where the CEA does not explicitly provide for the sharing of information (eg under an agreement), the disclosure of information is considered on a case-by-case basis taking into account the need to comply with the Privacy Act 2020 and the OIA. Principles in relation to maintaining commercial confidentiality are also applied.
20. The Privacy Act 2020 governs how organisations can collect, store, use and share personal information. In general, organisations must only collect information for a lawful purpose connected to their function, and only when necessary. Further, once that information is collected it must only be used for the purpose for which it was collected, unless an exception applies, as set out in principle 11 of the Privacy Act.
21. Additional uses of personal information, or disclosure of personal information except to the person it relates to, can only occur in certain circumstances. These are set out in Privacy

Principle 11 of the Privacy Act 2020. For example, and relevant to this RIS, personal information held by Customs can be disclosed to another agency or any person where Customs believes, on reasonable grounds, that disclosure is necessary to avoid prejudice to the maintenance of the law.

22. In some cases, there is a strong link between the need for personal information to be disclosed and the maintenance of the law (for example, Customs gives travel movements to the New Zealand Police for them to verify whether a person under investigation was in the country during the commission of a crime). Where the link between the disclosure and a clear law enforcement purpose is less obvious (for example, Customs providing interception information that may contain some personal information to SCP so that they can identify and address potential vulnerabilities in their supply chain) Customs is more likely to take a conservative approach in determining whether to disclose information, to avoid a potential privacy breach and the subsequent risk of reputational damage. The reluctance to disclose where the limits of disclosure are unclear means that opportunities to detect or prevent offending may be missed.

What is the policy problem or opportunity?

23. Customs and SCP need to work together to strengthen supply chains against TSOC, and insider threats especially. Two-way information sharing is central to achieving this objective. For example, information from SCP concerning breaches of their security systems would support improvements to Customs' border risk assessment and targeting activities, and information from Customs to SCP on interceptions of illicit commodities would assist SCP to identify and address vulnerabilities in their security systems and supply chains noting that they have a commercial imperative to maintain a corruption free, reliable supply chain. Information from Customs that would assist SCP to meet this objective may include personal information, for example consignor/consignee names and addresses from interceptions made at New Zealand's border.
24. Customs may also hold intelligence that indicates that a particular person is a border security risk due to the person's associations or history coupled with their holding a position in the supply chain or its supporting systems that could be used to facilitate TSOC activity. The sharing of this information with a CCA or other New Zealand based SCP where Customs reasonably believes there is heightened border security risk would enable risk mitigations to be made by the SCP.
25. Without information sharing, Customs and other SCP committed to combatting the TSOC threat will miss opportunities to detect, disrupt and deter illicit activity.
26. The problem is how to overcome the barriers to information sharing taking place, and to ensure that appropriate protections and restrictions are transparently applied when the sharing of personal information is involved. The principal presenting problems and issues are:
- how to establish an ongoing commitment to the sharing of information
 - how to give comfort to SCP (particularly those that might be sharing information sourced or held overseas) that information sharing by them is both legal and necessary and will not result in adverse or prejudicial outcomes for them
 - agreeing and enforcing limitations on how any information shared may be used, and acceptable standards for its storage, on-sharing, and disposal

- providing transparency where personal information may be shared and under what conditions, and how that relates to the information privacy principles established in the Privacy Act 2020.
27. The systematic and ongoing sharing of border security information to achieve border security objectives would achieve the most benefit in relation to larger and more diverse SCP, including those that operate internationally such as vessel/aircraft operators and international freight companies. The experience with overseas based SCP is when it comes to the sharing of sensitive information (including personal information) with an enforcement agency, that there is a reluctance to share because of a perceived risk of conflict with laws in the country where the information is held, and/or the information supplied may result in a prejudicial outcome such as a prosecution or an increased level of border intervention with their business activities. A formal legal arrangement is necessary to address these issues. Non-regulatory options such as a memorandum of understanding are not suitable.
28. The disclosure of personal information for the purposes of the maintenance of the law is enabled under the Privacy Act 2020. This requires consideration by the holder of the information on the application of the Privacy Act on a case-by-case basis, ie each time personal information is disclosed. In the case of irregular or one-off information sharing with SCP this enabling framework is sufficient to achieve border security objectives. In the case of the systematic and ongoing sharing of border security information, using the Privacy Act alone does not overcome all the barriers and issues identified in the problem definition.
29. Addressing the sort of issues discussed above lead to the establishment of a formalised information disclosure regime in the CEA in 2018 when it was reviewed and updated. However, the information disclosure regime as it applies to private sector organisations (section 317 CEA) is not suitable to apply to the particular circumstances needed to work with SCP to improve supply chain security and combat TSOC and the insider threat because agreements made under section 317:
- cannot operate on a two-way basis ie Customs to SCP **and** SCP to Customs
 - cannot be made with an overseas based private sector organisation
30. It is not explicit that an agreement made under section 317 can include personal information. Agreements can include information that would be released if requested under the OIA. Personal information can therefore be included if it would be released under the OIA ie where public interest in releasing the information is adjudged to outweigh the privacy interests of an individual.
31. Aside from these matters an agreement made under section 317 does address the principal presenting barriers to information sharing specified in the problem definition, in particular
- agreements are made at the chief executive level which creates an ongoing commitment to the sharing of information
 - agreements must specify matters such as the type of information that can be shared, the purposes for which it can be shared, the purposes for which it can be used and retained, and other relevant details (such as requirements relating to on-sharing, storage and disposal). This aspect reduces the risk of unauthorised disclosure, supports consistency in the application of protections over the information shared, and gives transparency to the information sharing. It also promotes administrative efficiency over case-by-case information sharing.

- As agreements are made under legislation, they can act as a means to assure participants that information sharing has a status that will minimise legal risk as long as the agreement is strictly adhered to.

What objectives are sought in relation to the policy problem?

32. The objective is to improve border security through the transparent, efficient, and proportionate sharing of border security risk information between Customs and SCP while ensuring the application of the principles of the Privacy Act 2020 to any personal information that is shared.

What consultation has been undertaken?

33. Customs has undertaken targeted engagement with SCP (including ports, airports, freight forwarders, and logistics companies). These stakeholders all indicated an awareness of and concern about the problems in information sharing for border security purposes and were supportive of an information sharing framework being established in the CEA. Targeted engagement was considered more appropriate, rather than wider public engagement, because the proposals primarily impact supply chain participants. Customs will continue to engage with industry stakeholders as legislation is developed and implemented.
34. Customs engaged with the following government agencies: the Department of Prime Minister and Cabinet, Ministry of Justice, Ministry of Business Innovation and Employment (Immigration Policy), New Zealand Security Intelligence Service, Government Communications Security Bureau, New Zealand Police, Ministry for Primary Industries, Ministry of Defence, and Te Puni Kōkiri.
35. Engagement with the Office of the Privacy Commissioner is ongoing.

Section 2: Assessing options to address the policy problem

What criteria will be used to compare options to the status quo?

36. The following criteria is used to compare options to the status quo:

- a. facilitation – enables better facilitation of information sharing between Customs and supply chain participants
- b. workable and efficient – able to be implemented and managed effectively and is the best use of resources
- c. reasonable – only enables information sharing powers that are considered within what is reasonably expected of Customs
- d. management of risk – enables better management of border security risks.

What scope were options considered within?

37. This RIS is focused on legislative clarity and enabling information sharing through modifications to an established legislative framework. For this reason, non-regulatory options were not explored as part of this analysis. For example, memoranda of understanding were rejected as an option as they are not a ‘means for sharing’ but a non-binding relationship agreement that outlines the basic terms of the agreement and records what information is being shared, who with and for what purpose. It does not authorise the sharing of information and all sharing of information must still be permitted under legislation, such as the CEA or the Privacy Act 2020.
38. An Approved Information Sharing Agreement (AISA) made under the Privacy Act 2020 was not considered as an option. This is because it is arguable as to whether an AISA with a SCP would fit within the authorised scope of ASIAs as set out in the Privacy Act 2020 - limited to “facilitate the provision of public services” (Privacy Act section 136), and also because an AISA cannot be made with an overseas based entity.
39. Information sharing for the purposes of the pre-employment vetting of staff or managers of CCA or SCP, or of directors for the purposes of licensing a CCA is out of scope. Vetting as a requirement of CCA licensing is discussed in a separate RIS prepared for the Customs and Excise (Border Security) Amendment Bill.

What options are being considered?

Option One – status quo

40. This option would mean facilitating systematic and ongoing sharing of supply chain security related information between Customs and SCP through the existing information disclosure regime in the CEA and through non-regulatory means such as memoranda of understanding. The Privacy Act 2020 would be applied on a case-by-case assessment when consideration is given to including personal information among any information to be shared.

Option Two – amend the CEA to clarify and enable two-way information sharing for border security purposes with supply chain participants

41. This option involves amendments to the CEA to enable systematic and ongoing sharing of supply chain security related information between Customs and SCP, and which

incorporates the essential features currently contained in the CEA's information disclosure regime.

42. The legislative features of this option would be:

- information sharing would be under an agreement made at the chief executive level between Customs and an individual private sector SCP
- agreements would be entered into voluntarily
- agreements may only be made for the purposes of supply chain and border security
- agreements would be limited to the two way exchange of specified supply chain integrity information. Information could include personal information, for example specified personal information held by Customs may be shared with a CCA or other New Zealand based SCP where Customs reasonably believes there is heightened border security risk posed by employees of, and those with access to, CCAs or other New Zealand based SCPs' facilities or operating systems
- to align with the CEA and with the New Zealand Information Sharing Standard⁶ agreements must specify:
 - o the particular type or class of information to be shared
 - o how the information may be used by the recipient
 - o the form in which the information is to be shared
 - o the positions or designations of the persons in each organisation with whom the information may be shared
 - o the safeguards that are to be applied for protecting personal information, or commercially sensitive information, that is shared
 - o the requirements relating to storage and disposal of information
 - o the circumstances (if any) in which the information may be disclosed by the recipient to any other agency or private sector organisation, and how that disclosure may be made
 - o the requirements for auditing and reviewing the agreement.

43. It is proposed that information shared under an agreement could not be used for a prejudicial purpose, such as a prosecution or for enforcement purposes, without the explicit agreement of the party that supplied the information.

44. For functional efficiency, it is proposed that a template agreement for New Zealand SCP will be developed in consultation with Office of the Privacy Commissioner, which will set the outer limits for any individual agreement. Discussion with the Office of the Privacy Commissioner is ongoing as to whether the CEA should require that the Privacy Commissioner should be formally consulted on each agreement with a domestic SCP prior to it being finalised.

⁶ This is the standard issued by the Government Chief Digital Officer for providing third parties with access to government held personal information. All public service agencies must implement this standard from 1 July 2025. See: www.digital.govt.nz/standards-and-guidance/information-sharing-standard.

45. Similar to section 318 of the CEA, the CEA will require the Privacy Commissioner be formally consulted as part of the process of making an agreement with overseas SCP that includes the possibility of sharing personal information.

PROACTIVELY RELEASED

How does the option compare to the status quo?

	Option One – Status quo	Option Two – amend the CEA to clarify and enable certain information sharing for border security purposes with supply chain participants
Facilitation	0 This relies on the enabling principles in the Privacy Act to enable information sharing when personal information is involved.	++ This will provide clear purposeful sharing of relevant border security information between Customs and a limited range of SCP through written agreements. This will facilitate increased trust and relationship between Customs and SCP, and enhance the integrity of the border and supply chain through effective information sharing.
Workable and efficient	0 In the case of irregular or one-off information sharing with SCP, this enabling framework is sufficient to achieve border security objectives. In the case of the systematic and ongoing sharing of border security information, using the Privacy Act alone does not overcome all the barriers and issues identified in the problem definition.	++ This option will require resources to establish procedures and put agreements in place. To keep this manageable and achievable within current resourcing, a targeted and risk-based approach will be taken to limit the number of SCP with which an agreement is made. It will ensure consistency with Privacy Act by ensuring disclosure of any personal information is undertaken consistently and transparently. It will facilitate a collaborative approach between supply chain participants towards the common goal, being the reduction or elimination of TSOC influence and intrusion into the supply chain. The fact that the ability to share information is put in place may have some deterrent effect as it will increase the likelihood of illicit activity being detected. It is likely to cause some behaviour disruption.
Reasonable	0 It would limit information sharing to the exception of preventing, detecting and prosecuting offences	++ This option proposes a reasonable approach compared with the status quo, whereby only information pertinent to protecting border security is shared between Customs and certain SCP. In respect of requiring the provision of information, including when necessary personal information, it builds on the principles in the Privacy Act which enable

	Option One – Status quo	Option Two – amend the CEA to clarify and enable certain information sharing for border security purposes with supply chain participants
		disclosure, however, legislates these to ensure any such disclosures which occur are consistent. It appropriately balances the right to privacy with sufficient checks and balances in order to effectively protect border security.
Management of risk	0 Given the deteriorating risk profile as evidenced by the global increase of TSOC in the supply chain, the status quo is likely to be increasingly inadequate to manage the risks.	++ This will enable targeted management of border security and supply chain risks. Two-way information sharing will enable SCP to use their resources and technology to effectively mitigate risks. It will also enable Customs to build intelligence, increase awareness of risks, and respond timely and effectively to identified risks.
Overall assessment	0 The status quo requires consideration by the holder of the information on the application of the Privacy Act on a case-by-case basis, ie each time personal information is disclosed. In the case of irregular or one-off information sharing with SCP this enabling framework is sufficient to achieve border security objectives. In the case of the systematic and ongoing sharing of border security information, using the Privacy Act alone is resource intensive and does not overcome all the barriers and issues identified in the problem definition.	++ This will provide a clear legislative basis for Customs and supply chain participants to share information relating to border security. This option provides a proportionate and balanced approach to combatting TSOC through information sharing in line with the expectations of Customs in terms of border security. Compared with the status quo, it is expected to assist in identifying and preventing TSOC activity earlier and more consistently across the supply chain. It will enable New Zealand to better contribute to global initiatives to combat TSOC. It may assist New Zealand to maintain its global ranking as a trusted trader. It is likely to improve risk targeting and intelligence.

Key:

++ much better than the status quo -- much worse than the status quo
 + better than the status quo - worse than the status quo
 0 about the same as the status quo

What option is likely to best address the problem, meet the policy objectives, and deliver the highest net benefits?

46. Option two is preferred as it will result in a clear improvement on the status quo, in terms of creating a framework to address the barriers and issues with regular ongoing two-way sharing of information for border security purposes and which facilitates Customs and SCP working together to deliver on the wider objective of more effective border security. It gives a means to establish an ongoing commitment to the sharing of information and will give comfort to SCP (particularly those that might be sharing information sourced or held overseas) that information sharing by them is supported legally and will not result in adverse or prejudicial outcomes for them. It would build off the approach contained in the CEA for information disclosure by Customs to private sector organisations based on written agreements that are voluntarily entered into at the chief executive level by the two parties.
47. Option two promotes efficiency in information sharing through clear specification in a written agreement of the scope of information shared and the conditions for sharing it, thus simplifying decision-making and supporting a more consistent approach over case-by-case consideration to the application of caveats and conditions.
48. Option two also gives a high level of transparency over any personal information being shared by requiring agreements to clearly specify limitations on how any information shared may be used, and the minimum acceptable standards for its storage, on-sharing, and disposal. Option two is assessed as providing a reasonable balance between an individual's right to privacy and achieving the broader societal benefits from improved border security

Is the Minister's preferred option in the Cabinet paper the same as the agency's preferred option in the RIS?

49. Yes.

Marginal costs and benefits of the preferred option

Affected groups	Comment	Impact	Evidence Certainty
Additional costs of the preferred option compared to taking no action			
Customs	One-off costs to make legislation, and update operational policies and procedures	Low	High
	Ongoing costs to maintain policies and procedures, and provide training.	Low	High. Customs does not expect additional resource will be required to support these functions. Implementation will be prioritised to target key SCP and take into account other priorities for resources across Customs.

	One-off and ongoing costs associated with putting in place and maintaining an information sharing agreement, including costs of monitoring and auditing.	Low. To ensure that agreements are not overly bureaucratic, time consuming and costly to develop, Customs proposes to develop a template agreement in consultation with the Office of the Privacy Commissioner. To keep demands manageable within current resourcing a targeted and risk-based approach will be taken to limit the number of SCPs with whom an agreement is made	High. Entering into an information sharing agreement will be voluntary and therefore each party will have the opportunity to assess the relative costs, benefits and impacts of an agreement as part of that decision process.
	Ongoing costs associated with justifying any information held and shared in the event of a complaint (for example, the resources spent responding to a complaint made to the Office of the Privacy Commissioner or some other relevant body, if an individual considers their privacy has been breached).	Low. The potential for information privacy breaches will be minimised through controls and processes already established within Customs to ensure compliance with the Privacy Act and to act on complaints.	Medium to High. Depends on the scope and amount of personal information proposed to be shared under an agreement. Agreements will not include the sharing of personal information where this is unnecessary to achieve objectives.
Supply Chain Participants	One-off and ongoing costs associated with putting in place and maintaining an information sharing agreement.	Low. There are expected to be minimal costs to SCP in sharing the information covered by an agreement. There may be some costs involved in the collation and provision of information, although these will be minimal as the information that will be included in an agreement is that ordinarily held by a business in a readily retrievable manner.	High. Entering into an information sharing agreement will be voluntary and therefore each party will have the opportunity to assess the relative costs, benefits and impacts of an agreement as part of that decision process.
Office of the Privacy Commissioner	Ongoing. Costs associated with reviewing and commenting on agreements and	Low. There are not expected to be a large number of agreements made - they will be prioritised to target key SCP. It is intended to create	Medium to High. Depends on the scope and amount of personal information proposed to be shared under an agreement. Individual

	responding to any complaints made to the Office of the Privacy Commissioner, if an individual considers their privacy has been breached.	a template agreement in consultation with the OPC which will act to manage ongoing engagement costs. The potential for information privacy breaches will be minimised through controls and processes already established within the parties to agreements to ensure compliance with the Privacy Act and to act on complaints.	agreements will not include the sharing of personal information where this is unnecessary to achieve objectives.
Non-monetised costs	One off and ongoing	Low	High
Additional benefits of the preferred option compared to taking no action			
Customs	Ongoing. Expected to generate improvements to Customs' border risk assessment and targeting activities.	Medium to high. It is expected that improved information sharing will contribute to both improved resilience of supply chains to TSOC activity and improved detection of and disruption to TSOC activities.	Medium. Information sharing is not an end in itself and the impact of an individual information sharing agreement on the wider objectives in relation to TSOC depends on the usefulness of the information shared and resulting follow up actions.
Supply Chain Participants	Ongoing. Expected to assist SCP to identify and address vulnerabilities in their security systems and supply chains.	Medium to High. TSOC infiltration of an individual business' supply chain tends to be a low frequency high impact event. Certain types of SCP such as international shipping companies and air and sea ports can be expected to face ongoing TSOC threats.	Medium to high. The value of an information sharing agreement to an individual SCP will be measured through the successful identification of vulnerabilities in their security systems and supply chains. It may have the indirect benefit of also assisting SCP to improve the safety of workplaces.
Government and those involved in international trade	Ongoing. Improved resilience of supply chains to TSOC threats will contribute to New Zealand maintaining its international reputation as a relatively corruption free and low risk trading partner.	Medium to High	Medium. The impact of individual information sharing agreement on wider government objectives in relation to TSOC is indirect.

Non-monetised benefits	Ongoing	Medium to High	Medium to high
-------------------------------	---------	----------------	----------------

50. There is confidence the proposal will achieve net benefits by facilitating and supporting two-way information sharing to generate improvements to Customs' border risk assessment and targeting activities and to assist SCP to identify and address vulnerabilities in their security systems and supply chains. It may have the indirect benefit of also assisting SCP to improve the safety of workplaces. Due to the variables involved the scale or quantity of benefits cannot be accurately measured and therefore have to be qualitatively assessed against the costs and impacts.
51. Information sharing is not an end in itself and the impact of an individual information sharing agreement on the wider objectives in relation to TSOC depends on the usefulness of the information shared and resulting follow up actions. The scale of the actual costs and harms being imposed on society by TSOC groups are high and so even a marginal increase in the deterrence, and detection and combatting of TSOC activity through information sharing will be beneficial if it can be achieved at low cost.
52. The wider benefits would come from the information shared contributing to actions that would:
 - a. prevent social harm through increased detection and disruption of TSOC activity in supply chains in such areas as the supply of illicit drugs to New Zealand
 - b. protect New Zealand's reputation and trusted trader status by tightening supply chain security through identifying and prosecuting trusted insider threats, and identifying, mitigating and managing border security risks.
53. The upfront and ongoing costs to Customs and an individual SCP associated with putting in place and maintaining an information sharing agreement are expected to be low, noting that entering into an information sharing agreement will be voluntary and therefore each party will have the opportunity to assess the relative costs, benefits and impacts of an agreement as part of that decision process. Given the feedback from industry during targeted engagement, it is considered this is a cost SCP are willing to accept in the interests of improving the resilience of their systems and contributing to improved border security.
54. It is not anticipated the proposed changes will negatively affect business competition.

Section 3: Delivering an option

How will the proposal be implemented?

55. The preferred option will be implemented through an amendment to the CEA that is expected to be in effect by late-2026.
56. Implementation will include the development of new information sharing agreements and standard operating procedures or guidance, which will require input from across Customs (including operations, policy, privacy and legal). This will be included in business-as-usual work for Customs and does not require additional funding. It is intended to create a template agreement in consultation with the Office of the Privacy Commissioner which will act to manage ongoing implementation and engagement costs.

How will the proposal be monitored, evaluated, and reviewed?

57. Under the proposed legislative framework, the new information sharing agreements will be required to establish an in-built audit and review process at the point of creation. This will ensure they are audited and reviewed at appropriate intervals, operating as intended, and are delivering the desired outcomes for all parties involved. The parties to the information sharing agreements will determine the appropriate frequency of these reviews and any indicators of success.
58. There are also overlapping requirements for oversight, including the information sharing standard issued by the Government Chief Digital Officer (which must be implemented by all public service agencies from 1 July 2025). This sets out a standard for providing non-government third parties with access to, or collection of, government-held personal information and been designed to protect personal information in that context.
59. The CEA is subject to Customs' ongoing regulatory stewardship function as the agency responsible for administration of the CEA.