INFORMATION

Customs' information framework and goals

AT A GLANCE

Having timely, accurate and relevant information enables Customs to protect the border while facilitating the movement of legitimate trade and travel.

Our goal is to develop a coherent, transparent framework for collecting, using, storing, sharing and disposing of information that:

- maintains and builds trust and confidence in the way that Customs collects, uses, stores, disposes and shares information
- maximises value for New Zealand from the information that we hold
- supports our principles for how we collect, use, store, dispose and share information.

Getting your feedback

We are interested in your views on how our framework for information can:

- support new ways of sharing information between government agencies to better protect New Zealand
- support the sharing of information within government for broader government purposes
- clarify our ability to share information with overseas agencies
- provide direction on when and how we share information outside of government
- provide guidance on how to treat commercially sensitive information
- ensure flexibility in the process for setting timeframes, and updating particular timeframes, for when Customs receives information
- ensure that personal travel records are protected.

Our role will remain the same

Customs provides essential border services and infrastructure that protect New Zealand and make our trade and travel more competitive in the global market.

The options we are considering for change to our information framework would not change this role or our functions, or those of other agencies.

> "Since 1996 travel volumes have doubled and trade volumes have increased seven-fold"

Information is essential to Customs

Worldwide, border agencies face a common problem: how to move legitimate travellers and goods across borders quickly and seamlessly while also protecting the integrity of the border by preventing unlawful people or goods from coming into the country.

Like our international counterparts, New Zealand Customs works in an environment where the way we work needs to keep up with the growing volumes of trade and travel. Since 1996 travel and trade volumes have increased dramatically:

Increase in travel and import volumes (1996/97 – 2013/14)		
	1996/97	**2013/14**
Passengers processed	5.4 million	11.2 million
Import transactions	1.0 million	7.8 million

This growth, which shows no sign of slowing, requires us to work faster so we don't slow down the trade and travel that is so critical to our economy. It also requires us to be smarter so that we can identify any goods or people that may pose a risk to New Zealand.

It is not easy to predict how many people, goods and craft crossing the border will break the law or how they will do this. We do know that those who seek to break the law will try to use legitimate means to cover their activities – such as hiding illegal items in a legitimate consignment of imported goods. Yet it is not realistic to try to check all goods, people and craft entering or leaving the country to find out whether they are complying with the law.

We expect the amount of information we receive to grow over time. In 2013/14 Customs received information about:

- 11.2 million travellers
- 10.3 million import and export transactions
- 945,910 import and export sea containers
- 4,948 commercial craft
- 1,223 small craft
- 198 cruise ships
- 454,000 arriving and departing passengers and crew from cruise ships.

Our response has been to develop an intelligence-led risk management approach to identify risks so we can achieve what we call "high assurance, light touch" – meaning that travellers and traders that present risks are identified early on and can be managed appropriately without holding up legitimate border traffic.

To help us identify risks we work closely with other government agencies to protect the border and New Zealand. Customs and other government agencies give and receive information to build a fuller picture of risk and help coordinate our agencies' responses.

Border agencies around the world are responding to the same challenges in a similar way.

To ensure we can respond effectively to changes in our environment, we continue to develop and refine our intelligence-led risk management model.

Information and trust

Intelligence-led risk management relies not just on good-quality information, but also on trust. We trust the majority of travellers and businesses to comply with border controls. In turn, trust is built on people and businesses providing us with accurate, timely and relevant information.

Who provides Customs with information?

- importers and exporters, including their intermediaries such as customs brokers, couriers and freight forwarders
- passengers of air and sea craft – for example, when they fill in a departure or arrival card
- owners and operators of air and sea craft, such as airlines
- domestic and international government agencies
- domestic businesses that produce goods subject to excise (alcohol, tobacco and transport fuels).

The types of information we collect

Information enables our intelligence-led risk management approach. Our unique position at the border also allows us to support other government agencies to manage risk and to meet New Zealand's wider international obligations.

Customs collects information on all goods, people, sea and air craft that cross the New Zealand border. We collect some information for our own purposes, while some we collect jointly with other government agencies, and some we collect for and on behalf of other government agencies. Customs, as a government department, is also legally required to create, maintain and dispose of records as part of normal, prudent business practice.

Overall, Customs acts as a custodian of a vast, and growing, amount of information for the New Zealand Government.

Examples of information collected by Customs

Information collected for Customs purposes:

- value and volume of goods
- origin of goods and craft
- destination of goods and craft
- identity of people crossing the border (New Zealanders and non-New Zealanders)
- prohibited and restricted goods
- intelligence on goods and people from domestic and government agencies
- excise-related information
- information from overseas agencies
- business records.

Information collected on behalf of other government agencies:

- identity of non-New Zealanders crossing the border
- border-crossing movements of New Zealanders
- goods subject to tariff duty
- anti-dumping
- countervailing duties
- prohibited and restricted goods
- origin of goods and craft.

Information collected jointly:

- goods and craft information submitted through the Joint Border Management System
- statistical information about people, goods and craft
- restricted goods (such as firearms).

Why information sharing is important

The information we collect and hold has value, not just for Customs, but for a range of government agencies. The information can be used to help manage security, support the maintenance of the law and, more broadly, to derive social and economic value in a variety of ways. For example, we have an information matching agreement with the Ministry of Justice to identify fine defaulters trying to leave New Zealand.

Another example of the value of Customs' information to other agencies is the use of our system to place "alerts" on people and goods crossing the border. An alert is when someone or something is flagged for attention when crossing the border – for example, a person whose parole conditions restrict them from travelling overseas.

> We have over 65,000 alerts on our system; 94 percent are for other

The environment in which we work has changed since 1996. Risks are constantly changing, while new technologies are allowing us to extract greater value from information to achieve government objectives such as greater customer segmentation or risk targeting. We are working in an environment that anticipates and encourages greater information sharing for public benefit, such as through the Better Public Services programme. And we are working in new ways ourselves – for example, by participating in special "operational coordination centres" for multi-agency activities.[2]

Making appropriate use of the information that Customs collects is an efficient way for the Government and others to achieve their goals. Information can be collected once and then shared, in clearly defined circumstances, to enable different agencies to perform their legitimate functions. An example is the Joint Border Management System developed by Customs and the Ministry for Primary Industries (MPI); under this new system businesses need only provide import/export information once, rather than separately to both Customs and MPI.

We discuss information sharing further from page 32 of this paper.

[2] Operational coordination centres are multi-agency teams that coordinate government activities in one place. Customs is the lead agency for two coordination centres – the Integrated Targeting and Operations Centre (often referred to as a "fusion centre") and the National Maritime Coordination Centre – and is a member of several others.

Our principles for managing information

Businesses and the travelling public trust Customs to deal appropriately with the information they provide to us. A 2013/14 survey showed that:

- 89 percent of commercial customers trusted Customs
- 89 percent of the travelling public trusted Customs.[3]

It is essential to our way of operating that we maintain and build upon this trust. Without trust we potentially undermine the provision of accurate information, which would not support our intelligence-led risk management approach to managing the border.

We use the principles set out below to support trust and confidence in the way that we collect, use, store, share and dispose of information. Our principles draw from and align with the Government's data and information management principles.[4]

Our principles governing how we collect, use, store, share, and dispose of information

Information is only collected, accessed, used and shared for clear, legally supported purposes.

- the information we collect is protected by appropriate ICT security measures (for example, our servers are built to Government Restricted level) and, for certain levels of information, access is restricted to designated Customs staff
- the information is protected from being unlawfully accessed or hacked
- if the information has been received from another government agency, it is protected in ways requested by that agency
- the information is protected from inappropriate access or use by users of our system, by the following measures:
    - there must be a clear purpose for access and sharing
    - people who are granted access are specifically identified and trained, and have the appropriate security clearances
    - access is traceable, audited with clear accountabilities for the access, use, storage and sharing of information
    - Customs carries out frequent risk and security audits (both internal and external) of our information databases.

[3] New Zealand Customs Service, *Annual Report 2013/14* p17 and p22.

[4] These principles can be found here: https://ict.govt.nz/guidance-and-resources/open-government/new-zealand-data-and-information-management-principles/

Our goal for our information framework

Our goal is to develop a coherent, transparent framework for collecting, using, storing, sharing and disposing of information that:

- maintains and builds trust and confidence in the way that Customs collects, uses, stores, shares, and disposes information
- maximises value for New Zealand from the information that we hold
- supports our principles for how we deal with information (see the previous page)
- ensures we have flexibility so that we can respond to changes in our operating environment – for example, new technologies and business practices
- ensures we receive accurate information and at the right time, preferably in advance
- ensures we collect the information we need in the most efficient and effective way.

We anticipate that some aspects of our information framework may be set out in Customs' new legislation, while other aspects may be dealt with in other legislation, such as the Privacy Act. Other features may be achieved as a result of Customs working better at an administrative or process level.

In developing the framework we need to ensure that Customs continues to be aligned with broader government frameworks and initiatives for managing and sharing information – for example, the New Zealand Data Futures Programme, the Better Public Services programme, and the Government ICT Strategy and Action Plan.[5]

Alignment will mean that we ensure any changes to our own information framework complement these broader initiatives. Key to this is ensuring that we align with and support the common thread that runs throughout the Government's frameworks and initiatives – namely, the aim of building public trust and confidence in government's ability to maintain the privacy and security of information.

OUR INFORMATION FRAMEWORK: WHAT DO YOU THINK?

Q 8 What are your views on Customs' principles for how we collect, use, store, share and dispose of information? Is anything missing? Should anything be added?

Q 9 What are your views on our goal for our information framework?

Q 10 What are your views on how we should ensure that our information framework aligns with broader government frameworks and initiatives for managing and sharing information?

[5] Information on these initiatives can be found on the following websites: www.nzdatafutures.org.nz; www.ssc.govt.nz/better-public-services; and https://ict.govt.nz/strategy/

Information sharing

Overall, our current legislative framework for sharing information is not transparent or coherent. Across the various regimes in the Act there is an inconsistent approach to handling information. Five specific issues are set out below.

From page 30 we discuss these five issues in the context of our principles for how we collect, use, store, share and dispose information and our goal for our legislative framework.

Terms used in this chapter

Information: we use this term to refer to both raw data (for example the elements of an import or export entry) and to information that provides context to data (who, what, when, where); and therefore makes it meaningful.

Personal information: information about an identifiable individual – for example, names and addresses of individuals. This includes biometric information (see page 56 for biometrics).

***Non-personal information*:** information that is not about an identifiable individual – for example, import or export information provided to us by a business. This information may be commercially sensitive.

Issue A: Difficulty supporting new ways of sharing information between government agencies to support the protection of New Zealand.

Issue C: International sharing provisions need to be clarified in two particular areas:

- information about goods
- the range of agencies we can share with internationally.

Issue B: Difficulty sharing information within government for broader government purposes.

Issue D: No explicit direction on sharing information outside of government.

Issue E: No guidance on how to protect commercially sensitive information.

Information sharing: The law as it stands

In our Act there are several specific regimes governing different types of information. The information Customs holds is also governed by the different regimes in the Privacy Act 1993, the Official Information Act 1982, the Public Records Act 2005 and, in some cases, other agencies' legislation.

Different rules apply to each of these regimes, dependent on the type of information, the information source, with whom we are sharing, or for what purpose we are sharing.

There are a range of rules in New Zealand legislation that determine:

- what type of information we can share
- with whom we can share the information
- the purpose of sharing the information.

The number of different information-sharing regimes can create lack of clarity about how Customs must deal with information – for example when regimes overlap and there is uncertainty about which regime to apply.

Nine of the different regimes that relate to Customs-held information are explained in the boxes below as examples (this is not an exhaustive list).

Joint Border Management System (JBMS)

JBMS applies to information about imported or exported goods that is provided to Customs or the Ministry for Primary Industries (MPI) by traders for border-clearance purposes. Both Customs and the MPI can access and use the information held in JBMS for their purposes.

When a request for information collected through JBMS is received from an agency other than the MPI, we consider the request under the principles of either the Official Information Act or the Privacy Act.

Personal information: Travel records and other

Information we hold about individual passengers will usually consist of personal information from different sources and is governed by two different Acts.

Information is governed by the Privacy Act if it has been collected from the passengers themselves when crossing the border (for example, the number of times they have crossed the border in a certain time period, or their destination), or during any interaction with Customs.

Information about the individual's travel that we have obtained from an airline is governed by the specific provisions in the Customs and Excise Act dealing with travel record information (see page 51).

When another agency asks us to share information we hold on a passenger, we need to first determine which legislation applies to the information, and then which legislation applies to the other agency.

Direct access to Customs' information database

The Police and the Security Intelligence Service (SIS) have the legislative authority to directly access our information database for counter-terrorism investigations until 1 April 2017 (due to a "sunset" clause in our Act). This permits them to log directly onto Customs' database, but they can only search it for information relevant to counter-terrorism investigations.

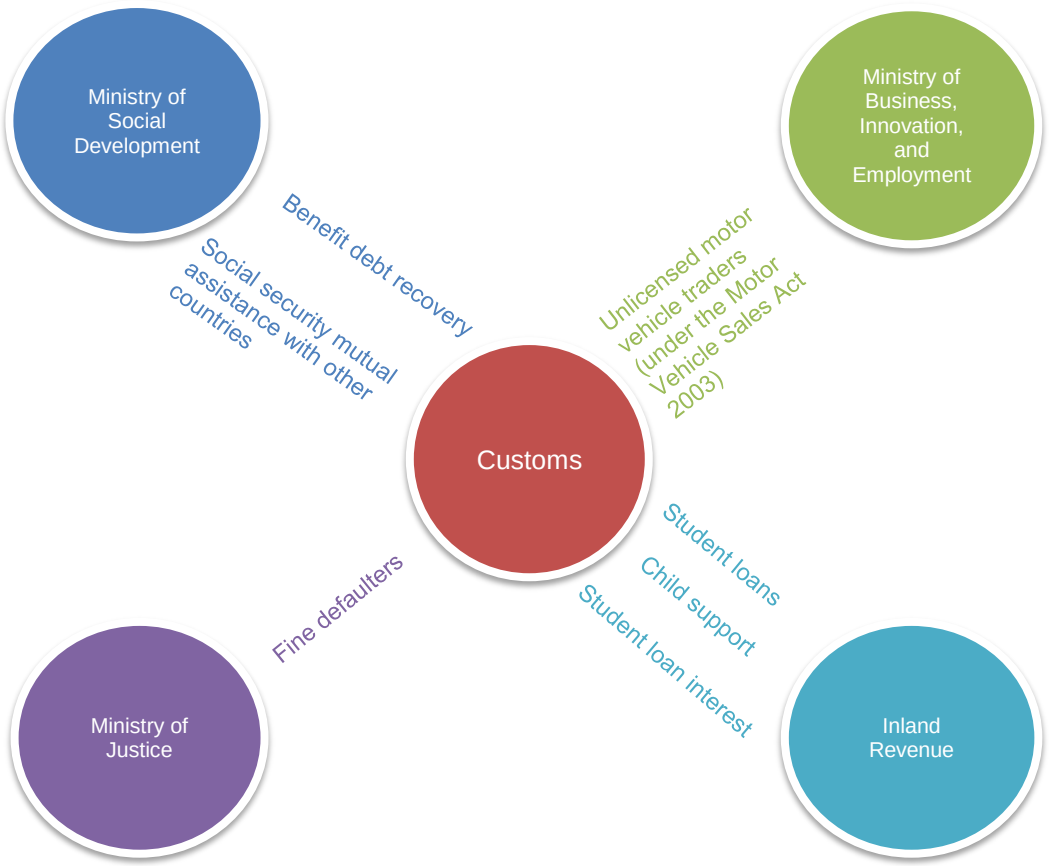
To guard against unwarranted or inappropriate access there are a number of procedural and administrative steps that must be followed to balance privacy and confidentiality issues. For example, before direct access is allowed, a written agreement must be developed between Customs, the Police and the SIS, and the Privacy Commissioner must also be consulted.

Information-matching programmes

The Customs and Excise Act sets out seven specific information-matching programmes. Information matching involves one agency matching its information datasets against another agency's to identify individuals appearing in both datasets. These programmes are governed by rules in the Privacy Act and are monitored by the Privacy Commissioner.

These programmes work well. We do not propose any changes to the provisions in the Act that govern these programmes.

Information Matching Programmes



Information sharing Regulations

The Act allows for Regulations to be made permitting Customs to enter into information-sharing agreements with other agencies that work at the border – for example, Immigration New Zealand and Maritime New Zealand – but only for border-protection purposes. These arrangements could include other border agencies having direct access to Customs' database.

This regulation-making power was added to the Act in 2012 in anticipation of substantial ongoing needs for new information-sharing arrangements relating to border security, particularly for the purposes of operational coordination centres such as the Integrated Targeting and Operations Centre (ITOC) and the National Maritime Coordination Centre. No Regulations have yet been made under this power.

International information sharing

Under Customs Cooperative Arrangements, New Zealand may be asked to share information with customs agencies overseas.

If their request is for personal information we are able to share it, with few limitations under the international information-sharing regime.

If the request concerns non-personal information on imports or exports, there is no guidance in our Act as to how we should protect this information.

Non-personal, commercially sensitive information

Different considerations apply to sharing non-personal information domestically. As there is no guidance in the Customs and Excise Act as to how Customs should treat commercially sensitive information, the approach we take is to treat it in accordance with the principles of the Official Information Act, and therefore protect it from disclosure when this would unreasonably prejudice the commercial position of the information supplier.

We recognise that much of the information that importers, exporters and their representatives are required to provide to us is commercially sensitive.

Sharing outside of government

Some industry bodies regularly request import or export data from Customs to assist them in providing services to their members. Currently we only give this data to these bodies if we have the consent of the individual importers or exporters.

Each request from outside of government is dealt with under the Official Information Act. That Act allows a maximum turn-around time of 20 working days for responding to a request.

The Customs and Excise Act gives no explicit directions on when and how Customs can share information outside of government, including with businesses and industry bodies.

Personal information: biometrics

Our current Act does not explicitly deal with the collection, use, storage, sharing and disposal of biometric information.

This topic is discussed in a separate chapter at page 56.

Information sharing: Key issues and opportunities

We believe that our current legislative framework for information sharing is not transparent or coherent. There is an inconsistent approach to the handling of information across the various regimes, as explained above. Given the changes that have occurred in technology, business practices and government priorities and expectations, we do not believe we can carry out our functions effectively without changes to the current legislation in this area.

In particular, we have identified that our current legislative framework:

- may not adequately support new ways of sharing information between government agencies for the purpose of protecting New Zealand
- may not adequately anticipate possible needs for sharing information within government for government purposes other than border protection and law enforcement
- needs to clarify the types of information that can be shared with overseas agencies, and with which overseas agencies
- gives no explicit directions on when and how to share information outside of government
- provides no guidance on how to treat commercially sensitive information.

The issue of biometric information (which is a form of personal information), and of how our legislative framework deals with this information, is dealt with separately from page 56.

Issue A: Sharing information with security and law enforcement agencies

Our legislative framework does not support new ways of working with non-border agencies for purposes other than border protection, particularly in operational coordination centres such as the Integrated Targeting and Operations Centre (ITOC).

Within centres like ITOC, staff from several agencies are located together for quick, easy cooperation between agencies for joint purposes. Staff can access their own agency's information systems and share information in accordance with the existing law to coordinate multi-agency operations.

ITOC and other operational centres have significantly increased the level of cooperation between agencies, within the limitations of the existing legislative framework.

However, the way in which understanding risk works means that the traditional way of sharing information, through formal information requests from one agency to another in the same room, could be improved on by allowing other agencies to have direct access to Customs' information in some situations. This would allow government to extract the full potential value of Customs' information for purposes beyond border protection.

Advantages of direct access

To protect New Zealand, government agencies need to understand potential risk. To assess risk it is not enough to look only at one piece of information – agencies need to lawfully access and put together multiple pieces of information to develop a richer picture of risk. However, not all this information will come from one agency's information system. Sometimes it is by accessing information held by other agencies that an insight can be developed into the risk posed by someone or something crossing the border. Accessing information in this way can also help government agencies identify risks that they did not know existed.

We believe that in some situations allowing other government agencies to directly access our information, for specific purposes (such as law enforcement, national security and border protection), is an effective and efficient way to work.

Located in Auckland, the Integrated Targeting and Operations Centre (ITOC) is New Zealand's border operations connection to the world, 24 hours a day, 7 days a week.

Agencies in the ITOC are: Customs, the Ministry for Primary Industries, Immigration New Zealand (Ministry of Business, Innovation, and Employment), Maritime New Zealand, the New Zealand Police, Aviation Security (part of the Civil Aviation Authority), and the Security Intelligence Service.

For sharing information within ITOC:

- two agencies can directly access our information but only for counter-terrorism purposes
- the Ministry for Primary Industries can directly access JBMS for border purposes
- all other requests for information must follow a formal request process on a case-by-case basis.

A scenario of how information sharing can help in understanding risk

A person uses cash to buy a ticket to travel to New Zealand two days before travel. The way the ticket was bought and when it was bought could indicate criminal activity, or it could simply indicate rushed travel plans due, for example, to a death in the family.

To understand the risk posed here, government agencies would need access to information such as previous travel history, criminal records, and known associates. Government agencies might also need to question the traveller directly.

Direct access may allow an agency to quickly piece together all relevant information rather than relying on each agency separately identifying and requesting information. It may also allow an agency to make connections between people and goods and identify investigative opportunities that would not be apparent otherwise.

Relying on Customs to provide agencies such as the Police with information to help protect New Zealand creates a risk that relevant information will be overlooked, especially as Customs would be unlikely to have the contextual understanding to know whether the information is relevant.

Direct access can also remove time-lags and reduce the resource costs of accessing information. For example, at the moment the Police are only authorised to directly access our information to create or amend border alerts and to search for information for counter-terrorism purposes. If they want to check whether someone is in New Zealand they must prepare a request asking Customs for this information, and we must then assess the validity of the request against the Privacy Act. If we decide the request is necessary, we check in our databases and then inform the Police officer of the outcome of our search. A brief query may turn into a lengthy process and the Police still may not get the information they are looking for.

A scenario of how direct access could help protect New Zealand

Police have concerns about illegal weapons in a particular house. Specific Police officers, who have the appropriate training and security clearances, are able to directly access Customs' information.

They find that we hold information about a person of interest to the Police – a known high-level organiser of illegal weapons trading and a close associate of the occupant of the house in question. Our information tells them that this person has just left New Zealand. This ties in with information the Police have that a weapons deal is taking place as soon as the organiser leaves, and it enables the Police to immediately start operational planning for their response.

Here, direct access to Customs' information saves the Police time, and also helps them to link people together and build a picture of potential criminal activity.

Risks involved with direct access

We recognise that direct access also carries risk in the form of potential for inappropriate access and sharing of information. This could happen if the allowable purposes for access are not clear, or if the security and protection settings are not clear or are not followed consistently.

Issue B: Sharing information with government agencies for broader government purposes

Increasing recognition of the value of Customs' information is meaning higher numbers of information requests from other government agencies. For example, while in 2008/09 we received 89 of these requests, in 2013/14 this had increased to 164. This figure does not

include the formal requests for information in centres such as ITOC (discussed above) or requests that were not made because they were not permitted under the current legislation.

We believe that the current legislative framework for sharing information for broader government purposes could be improved so that greater value is extracted from Customs' information to support purposes beyond border protection.

We have identified some examples of where there could be some benefit in sharing information with other agencies:

Examples of sharing for broader government purposes

For regulatory compliance purposes: If the Energy Efficiency and Conservation Authority (EECA) were provided with information on product imports, this could help them:

- verify the information that importers provide to them directly
- ensure that all importers are aware of their obligations under the EECA's regulatory regime, and
- determine whether there is a need to regulate new classes of products for energy efficiency, and what the impact of regulating new classes would be.

For trade promotion purposes: If Customs shared information on exporters and importers with the Ministry of Foreign Affairs and Trade, the Ministry could consult with those traders on the negotiation of Free Trade Agreements and inform relevant traders about regulatory changes in other countries.

For service delivery: The Ministry of Transport collects information on freight through surveys of business, but some of this information is already collected by Customs. If Customs could share this information with the Ministry of Transport, this could reduce the compliance burden on business.

For revenue: Sharing excise or duty information with Inland Revenue could provide them with a broader tax picture.

This is only an initial list, and we believe there could be value in exploring this further. We would like your feedback on whether there is value in us sharing information more broadly than just for border protection purposes, and what those additional purposes should be.

Issue C: Sharing information with overseas agencies

International cooperation is vital to protect citizens from cross-border risks, to assist in response to natural or human-made crises, and to support economic growth through more effective movement of goods and people to and from New Zealand. This is why Customs has authority to share information with overseas agencies (including a number of international agencies, such as the World Customs Organization).

Current international information sharing

Customs works closely with international partners to combat crime, including in the areas of people-smuggling, drug-smuggling, terrorism, objectionable material, and cyber-crime.

Our current international information-sharing capability works well and enables us to cooperate with our overseas partner agencies. We are therefore not proposing substantive changes to the legislative framework for this type of sharing. We do, however, think that two specific areas need to be clarified:

- the types of information Customs can share internationally, and
- the types of overseas agencies Customs can share information with (by overseas agencies we mean here not just agencies of foreign governments but also international organisations that are part of the worldwide customs regulatory system, such as the World Customs Organization or the World Trade Organization).

The Customs and Excise Act does not specifically include non-personal information – such as information on imports and exports – as part of the information that Customs can share internationally, except where this is covered by a treaty, agreement or arrangement concluded by our Government. However, facilitating international trade is a key part of Customs' role.

> "Customs has a role in health protection, such as preventing and responding to pandemics, including the recent outbreak of Ebola, and the spread of avian/swine influenza"

In addition, the provisions for sharing with overseas agencies are inconsistent and have not kept pace with changes in Customs' role.

For example, the Act permits us to share travel records with overseas agencies whose functions include protecting public health and safety (see page 33). However, the Act does not permit us to share information other than travel records with those same overseas agencies.

We think Customs' legislation should clarify that Customs can share all relevant information with an agency who meets specific criteria set out in the Act, and those criteria should incorporate a broader range of agencies.

Issue D: Sharing information outside government

As with sharing within government, our interest in sharing with non-government organisations is to ensure we act appropriately as information custodians. We want a framework for information sharing that, among other things, allows value to be derived from the information we hold, and that builds **trust and confidence** in the way we deal with information.

The Customs and Excise Act gives no explicit directions as to when and how Customs can share information outside of government - for example, with businesses and industry bodies. This does not support transparency, and potentially undermines trust and confidence in Customs.

As with our current ability to share information with most government agencies, each request from outside of government must be treated case by case in accordance with the Customs and Excise Act, the Privacy Act and the Official Information Act.

Formal information sharing arrangements with bodies outside of government could produce further value for New Zealand from the information Customs holds. Specifically they could:

- reduce the burden on Customs by removing the need to respond to numerous individual requests for information under the Official Information Act (we currently deal with over 200 trade-related requests each year)
- improve our service to bodies outside of government by potentially speeding up our responses to information requests
- reduce costs for industry bodies and their members by making regular flows of information more systematic and timely.

One example of potentially reducing costs for industry is if we had systematic sharing with port companies. We currently have no guidance on whether we can enter into an agreement to share non-personal commercial information with organisations such as port companies.

Example: Sharing with port companies

Port companies collect information from traders, which is similar to information those traders must provide to Customs – for example, container numbers, shipper details, and the port of loading. There could be benefit in traders providing the information once only, to Customs, and Customs then sharing that information with the port company. This could reduce costs for the trader and possibly the port company.

Issue E: Protecting commercially sensitive information

All those who deal with information, including government agencies, are expected to apply appropriate protections for the information.

Personal information is protected through the Privacy Act. However, there is no legislative guidance on how Customs should protect non-personal, commercially sensitive information. The Customs and Excise Act is silent on what commercially sensitive information is and how we should deal with it. (However, Customs can withhold information requested under the Official Information Act if releasing it would unreasonably prejudice the commercial position of the supplier or subject of the information and if there is no overriding public interest in releasing it.)

Possible solutions for sharing information

We are considering two options. We prefer the first option and are interested in your feedback.

We believe our preferred option below would contribute to achieving our goal for our information framework (this goal is set out on page 31). Under this option our functions would not change, nor would those of other government agencies.

Our preferred solution: Create a transparent, coherent framework for sharing information

This option would establish a transparent, coherent framework for Customs to share more information with more government and non-government agencies. We are open to what practical arrangements the framework would involve. We want to ensure that it achieves our information framework goal (see page 34) and, more specifically, that it:

- allows for direct access to Customs' information for specified agencies for the purposes of law enforcement, national security and border protection
- provides a process to follow for sharing information for broader government purposes
- records information-matching programmes that relate to information held by Customs
- provides a process to follow for sharing of information internationally
- provides a process to follow for sharing of information outside of government
- respects our wider international obligations.

The framework would also give us a process for sharing biometric information (biometrics are discussed in detail from page 56).

We expect that some aspects of a new information sharing framework might be set out in our legislation, while other aspects may rest in other legislation, and some aspects may be achieved as a result of us working smarter at an administrative or process level. Before we work through the detail of how the framework might work we want to get feedback on what the framework should aim to achieve.

We recognise that this option requires careful thought about how Customs will maintain the trust and confidence of businesses and the public in how information is shared, at the same time as we maximise value for New Zealand from our information.

We need to consider whether our principles for how we collect, use, store, share and dispose of information need to be expanded to include, for example, whether consultation requirements need to be explicit in the legislation, or whether access to our information database should be ring-fenced to protect certain "pools" of information.

Summary of issues under this preferred solution

Issue	Solution
Issue A: Difficulty supporting new ways of sharing information between government agencies to support the protection of New Zealand.	Allow direct access by specific agencies to our information for law enforcement, national security and border protection purposes.
Issue B: Difficulty sharing information within government for broader government purposes.	Include a wider range of purposes in the Act, such as regulatory compliance, trade promotion, revenue and service delivery.
Issue C: International sharing provisions need to be clarified in two particular areas: • information about goods • the range of agencies we can share with internationally.	Expand our information sharing with overseas agencies to include: • goods and revenue information • a wider range of agencies.
Issue D: No explicit direction on sharing information outside of government.	Provide an explicit process in the Act for sharing information outside government.
Issue E: No guidance on how to protect commercially sensitive information.	Include a process in the Act for protecting non-personal, commercially sensitive information.

Issue A: Direct access for law enforcement, national security and border protection

Customs' legislation could be changed so that Customs could allow specified agencies to directly access our systems on an ongoing basis for law enforcement, national security and border protection purposes. This would formalise direct access by the Police and the Security Intelligence Service for counterterrorism investigations beyond the current sunset clause of 1 April 2017. It would also broaden the reasons for access.

To maintain trust and confidence in our protection of information, the development of a process for direct access would need to address potential risks, such as inappropriate access and sharing. Direct access should be restricted to identified and trained people with appropriate security clearances and it should only take place in a secure environment. Access would also need to be auditable and traceable. We expect that the development of an appropriate process will require consultation with the Privacy Commissioner, the Ombudsman, and affected parties.

We believe our principles for how we deal with information could be used in addressing the risks of direct access. We would like your feedback on whether these principles are robust enough to manage this risk and whether there are other protections we also need to consider.

Issue B: Sharing with government agencies for broader government purposes

We have identified a range of different government purposes, beyond border protection, for sharing Customs information. We would like your feedback on those purposes, and on whether there are other purposes we should consider.

These are some of the purposes we have identified:

- **regulatory compliance:** this could permit sharing to support regulatory regimes run by other agencies
- **trade promotion:** this could permit sharing to support the government's broader economic growth objectives
- **revenue:** this could permit sharing to support Inland Revenue's broader revenue function
- **service delivery:** this could permit sharing of information with agencies to help them improve their services to their customers and clients.

This information sharing would need to be consistent with our information principles (set out on page 30) and may also require consultation with the Privacy Commissioner, the Ombudsman, and affected parties.

Issue C: Expanding our information sharing with overseas agencies

The information sharing framework would provide a process to follow for sharing information internationally in accordance with our international obligations.

Two ways of improving our information-sharing internationally would be to:

- explicitly permit goods and revenue information to be shared with overseas agencies
- permit Customs to share with a greater range of overseas agencies, with the types of agencies being specified.

These changes would contribute to our reputation as a trusted international partner and improve our ability to support collaborative border management around the world.

Issue D: Sharing information outside of government

The framework would provide an explicit process for information-sharing with non-government agencies and organisations. The process would need to be consistent with Customs' principles for dealing with information and would require consultation with the Privacy Commissioner, the Ombudsman, and affected parties about possible "opt in" and "opt out" alternatives.

Issue E: Protecting commercially sensitive information

We could include a process for protecting non-personal commercial information in our legislation. This could reduce uncertainty, and build trust and confidence, as to how Customs manages the commercial information we hold.

Other solutions we are considering

Status quo

The second option is for Customs to retain our current legislative framework for sharing information, as set out from page 33. This would mean retaining and continuing to operate under the multiple information-sharing regimes in the Act, along with the Privacy Act, the Official Information Act, and, in some cases, other agencies' legislation.

We are concerned that this option does not provide us with the transparency we want in order to build trust and confidence in how we treat information. We also may not extract maximum value from the information that Customs holds for the benefit of New Zealand.

However, we would maintain our commitment to our principles for how we collect, use, store, share and dispose of information.

Who would be affected by change

Changes to the way we share information could affect all people and businesses that provide Customs with information. This includes traders, travellers, and excise manufacturers. Each of these customers' information could be subject to different information sharing mechanisms and could potentially be shared with more agencies for broader government purposes. Any changes would not affect the principles we use to manage the information provided to us though and the information will continue to be subject to protections where appropriate.

Such changes may also reduce compliance costs for individuals and businesses that may provide their information to fewer agencies. We are interested in hearing whether changes to our information sharing regimes could result in different compliance costs for you or your business.

INFORMATION SHARING: WHAT DO YOU THINK?

Q 11 What are your views on how our legislative framework for information works now? Do you see any tensions or uncertainty in how we deal with information in general or, more specifically, with the information that you provide to us?

Q 12 What are your views on how we could improve our legislation or our administrative processes to achieve our goal for information sharing?

Q 13 What are your views on Customs allowing specified government agencies to directly access our information for the purposes of law enforcement, national security, and border protection? Are our principles for how we collect, use, store, share and dispose of information robust enough to address the risks associated with direct access? Are there other protections we should consider for direct access specifically?

Q 14 Should Customs share information with government agencies for broader government purposes beyond border protection? Please give your reasons.

Q 15 Should Customs share information about goods internationally and with a broader range of overseas agencies? Please give your reasons.

Q 16 Should our Act provide an explicit process for Customs to share information with non-government bodies? Please give your reasons.

Q 17 How should Customs protect non-personal, commercially sensitive information? Should protection be through our legislative framework or through other means?

Q 18 What concerns do you have about allowing more sharing of the information that Customs holds? How could those issues be managed?

Q 19 What benefits do you see in greater information sharing? In particular, do you see any opportunities for you or your business or organisation?

Receiving and accessing information

We believe that our current framework for receiving and accessing information could be improved in two specific areas:

- providing flexibility in the setting of timeframes, and in the updating of particular timeframes, for when traders and travellers must provide Customs with information
- reviewing the protections for travel records.

Customs has considered these issues in the context of our principles for how we deal with information (see page 30) and our goal for our legislative information framework (see page 31).

The two areas of potential improvement identified above are considered in more detail in the following pages.

Timeframes for providing information

The law prescribes certain timeframes for providing Customs with information. However, because of the following developments some timeframes may no longer be practical or may not support our risk-assessment and other functions:

- most information is now provided to Customs electronically, and well within or in advance of the prescribed timeframe (some timeframes have not been changed since information was required to be sent by post)
- changes in business practices have created faster supply chains and faster transporting of goods
- changes in risks at the border post-9/11, and increases in the volume of people and goods crossing the border, have meant that border agencies now rely more heavily on timely and accurate information to ensure we can perform our risk-management functions.

Customs now receives more electronic information more quickly, and can process that information faster than ever before.

Some of the current timeframes were originally designed for a mainly paper-based system that provided little opportunity for advanced risk-management methods. Now, Customs is an intelligence-led agency with significant capability to target individuals and businesses that are illegally operating at the border and in revenue-collection areas.

Currently timeframes are set by regulation. We would like to confirm whether this process is fit for purpose and flexible enough to deal with future developments, or whether there are other options for setting timeframes that

> “The Customs and Excise Regulations 1996 prescribe 26 timeframes for different types of information to be provided to Customs”

we should consider that would be more flexible yet still able to provide adequate certainty to those who provide us with information.

We are not proposing any changes to the types of information that Customs receives.

Solutions we are considering

The suggested changes to timeframes that we are considering (see below) relate only to marine craft, goods entries, and claiming imported goods, not to aircraft and airline information. Airlines face quick turnarounds and Customs believes that that information is already provided in the most efficient way.

The options we are considering for timeframes for marine craft and cargo are as follows:

- **maintain the status quo:** timeframes would be unchanged for providing information to Customs
- **change timeframes:** whether timeframes would be changed so that Customs received the information earlier or later would depend on the specific requirement. For example:
    - requiring information to be provided to Customs earlier rather than later will allow us to target our risk assessment more effectively and ensure threats are managed. In most cases, information is already available earlier than the prescribed timeframes.
    - allowing businesses to provide information to Customs later will be more responsive to business practices, including better reflecting the speed of modern supply chains. However, this needs to be balanced against allowing adequate time for Customs to carry out risk assessments and maintain control at the border.

Customs' indicative options for the setting of timeframes are shown in the table on the following page:

Indicative options for the setting of timeframes

Requirement	Direction of travel/trade	Status quo: current timeframes	Indicative options
Advance Notice of Arrival (sea)	Incoming	Not less than 48 hours before arrival	Status quo; or An earlier timeframe of up to 72 hours before arrival
Advance Notice of Departure (sea)	Outgoing	Not less than 4 hours before departure	Status quo; or An earlier timeframe of up to 12 hours before departure
Inward Cargo Report (sea)	Incoming	Not less than 48 hours before arrival	Status quo; or An earlier timeframe of up to 72 hours before arrival
Outward Cargo Report (sea)	Outgoing	For cargo that is ½ not in bulk: 48 hours after departure For cargo that is more than ½ in bulk: 24 hours after departure	Status quo; or An earlier timeframe of up to the time of departure
Inward Report (sea)	Incoming	Within 24 hours of arriving	Status quo; or An earlier timeframe of up to 12 hours of arriving
Import Entry	Incoming	Standard: within 20 days after arrival For goods that are for transportation in New Zealand or removal for export where further entry is required: within 20 working days after first entry	Status quo; or An earlier timeframe so the import entry is submitted on or shortly before arrival
Export Entry	Outgoing	48 hours before departure	Status quo; or A later timeframe of up to 12 hours before departure
Claiming imported goods	Incoming	3 months to claim imported goods	Status quo; or Reduce the timeframe, for example up to one month

Who would be affected by change

If changes are made to the timeframes and processes for providing information to Customs, then all businesses and individuals that provide information would be affected – this includes ship operators, shipping lines, cargo operators, ports, importers, exporters and other associated businesses.

There may be some additional compliance requirements or costs for these groups as a result of changes to particular timeframes. We are interested in hearing from businesses about whether different timeframes would be practical, and on how significant they think any additional requirements or costs would be.

TIMEFRAMES FOR PROVIDING INFORMATION: WHAT DO YOU THINK?

Q 20 Do you agree that the current process of setting timeframes by Regulation is fit for purpose and flexible enough to accommodate future developments? Please give your reasons. What other processes could we consider, and why?

Q 21 Are all the indicated options for changes to timeframes practical? (Please see the column “Indicative options” in the table on page 49).

Q 22 Are there other timeframes that we have not considered that you think need to change?

Q 23 How would changes to timeframes for providing information affect you or your business?

Q 24 Would your compliance costs be higher or lower if timeframes were changed? If so, what would your costs be, and how significant would the increase or reduction be for you?

Reviewing the protections for travel records

International standards provide airlines with guidance on how to provide passenger information to border agencies worldwide. Passenger Name Record information is created by airlines and is governed by international standards that apply to all countries receiving Passenger Name Record information.

What are Passenger Name Records?

The Customs and Excise Act requires airlines to provide Customs with information on people crossing the border.

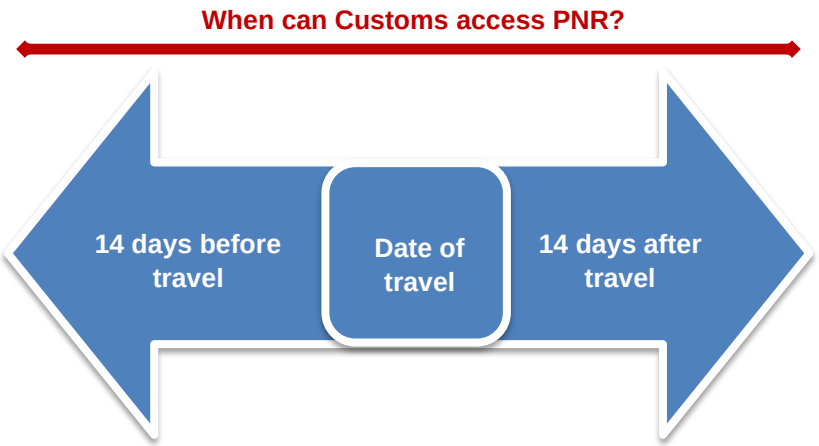
Customs receives this information in the form of Passenger Name Records. This includes personal information about passengers, such as their ticketing details.

Passenger Name Records are one of the main forms of information used by Customs to assess the risk that air passengers could pose to New Zealand, so we can intervene where appropriate. It is a key tool in our investigations into transnational criminal activity.

How Customs currently accesses travel records (the "pull" system)

Passenger Name Record information is currently provided by airlines to Customs by allowing us to access parts of their reservation systems and to "pull" the relevant information.

The Customs and Excise Act currently contains protections around Passenger Name Records based on the "pull" method of access. One of the most significant is that the information can only be accessed by Customs within 14 days either side of travel (28 days in total). For example, if a passenger books a flight six months before their travel date, Customs cannot access his or her booking information until 14 days before the travel date.



If Customs needs to view the information outside this timeframe, we must apply for, and obtain, a warrant from a District Court Judge.

A new automatic "push" system for travel records

The World Customs Organization, the International Civil Aviation Organization, and the International Air Transport Association have jointly developed guidelines recommending that Passenger Name Records be automatically sent by airlines to governments (called "pushing" the information) in a standard electronic format.

This new system is expected to be in place later in 2015. Customs will then no longer need to access airline databases for this information, as it will be systematically provided to us by airlines. The information will be available to us from 72 hours before the relevant flight departs. We will store the information securely and dispose of it once it is no longer necessary for Customs' purposes.

The Ministry of Business, Innovation, and Employment (MBIE) is currently progressing an amendment to the Immigration Act that would accommodate the changes to the way in which Passenger Name Record information is provided to Immigration New Zealand under the "push" system. This would include removing the 28-day window for access.

In the context of the new "push" system and those proposed Immigration Act changes, Customs would like to discuss the most appropriate mechanisms for protecting Passenger Name Record information while at the same time having access to the information we need to protect New Zealand's border, when we need it. In particular we would like to discuss whether the 28-day window for accessing airlines' Passenger Name Records should be retained.

How Customs uses historic travel information

Organised crime syndicates, transnational trafficking groups and terrorist networks are often extremely resilient. These organisations are very conscious of law enforcement techniques and are adaptable. Work by agencies, such as Customs, to build an accurate intelligence picture of these groups can therefore extend over a number of years.

Previous Passenger Name Record information can be used specifically to identify syndicate members, travel companions, previous drug couriers, previous travel patterns, and links to travel and drug shipments. This information can help Customs to investigate and prosecute criminal offending.

We also want to explore whether a warrant to access information in certain situations is still an appropriate protection under the new "push" system, or whether there are other protections we should consider.

If a court warrant is still an appropriate form of protection, we want to consider when it would apply and what the process for obtaining a warrant should be.

Our preferred solution: Remove the 28-day window for accessing travel records, and consider additional protections

Customs' preferred option is to remove the 28-day window for accessing Passenger Name Record information. This would reflect the changes in the way Customs will receive this information from airlines, and it would be consistent with MBIE's proposed changes to the Immigration Act. Customs would receive the information 72 hours before travel, and store it securely and only for as long as is necessary. There would be no restriction on accessing the information in the airlines' reservations system when this is necessary at other times.

For this option to be effective, we need to consider the impact on the current need for a court warrant to request Passenger Name Record information from airlines outside of the 28 day window. Taking into account the "push" system for receiving the information, and if there is no restriction on accessing the information when otherwise necessary, we see no circumstances in which a court warrant would be formally required under this option.

However, we will need to consider whether there are other protections that might be put in place around accessing, storing and disposing of the information, to ensure that these processes are consistent with our goal and principles for managing information (see pages 30 and 31).

Other solutions we are considering

Change the window for accessing travel records and consider whether warrants should still be required in some cases

This option would retain a window for accessing Passenger Name Record information **before** the date of travel. There would be no restriction on accessing Passenger Name Records after the date of travel, as Customs would already have received this information from the airlines under the new "push" system.

There will need to be a process for obtaining access outside of the window (that is, before the window period begins) when necessary. Customs would need to consider whether applying for a District Court warrant is still an appropriate process.

Again, we would need to consider whether there are other protections that might be put in place around accessing, storing and disposing of the information.

Continuing the status quo

The status quo would retain the 28-day window (14 days either side of travel) on Customs' accessing Passenger Name Record information, and the need to obtain a District Court warrant for access outside of that 28-day window. However, this could sit uncomfortably with the new internationally agreed system for managing this information once it is introduced later in 2015.

Who would be affected by the change

There would be no additional compliance costs or requirements for airline passengers or airlines. The information would be provided by passengers to airlines in the normal way, and airlines would provide Customs with the information through the new systematic "push" approach without change.

RECEIVING AND ACCESSING INFORMATION: WHAT DO YOU THINK?

Q 25 What protections do you think should be required for Passenger Name Record information?

Q 26 What are your views on our preferred option to remove from the Customs and Excise Act the 28-day window for accessing Passenger Name Record information?

Q 27 How would you be affected if the 28-day window were removed or changed?

Q 28 Do you think the requirement to obtain a District Court warrant would still be a necessary protection under the new "push" system described above? In what situations, if any, should a warrant be required? Are there other measures Customs should be considering to protect Passenger Name Record information?