

Te Tomokanga
**Primary line web applications and
secondary line web applications**
New Zealand Traveller Declaration
PRIVACY IMPACT ASSESSMENT

July 2023

V1.2

Product owners:



PROACTIVELY RELEASED

Contents

Document management.....	2
Version history	2
Distribution list for external distribution.....	2
Glossary.....	3
1. Introduction and purpose	7
2. PIA scope.....	13
3. Executive risk summary	13
4. Openness and transparency	14
5. Personal information to be captured	14
6. Assessment of privacy impacts.....	15
6.1 Collection of personal information.....	15
6.2 Storage and security	19
6.3 Access, correction and accuracy.....	20
6.4 Retention, use and disclosure	22
6.5 Offshoring of information.....	26
6.6 Unique identifiers	27
7. Risk, consultation and signature.....	27
7.1 Consultation	27
7.2 Signatures	27
Appendix 1 – Te Tomokanga processing flow	28
Appendix 2 – MPI search process flow.....	29
Appendix 3 – Project Risks and Controls table	30
Appendix 4 – Changes since version 1.1.....	34

PROACTIVELY RELEASED

Document management

Version history

Version	Date	Author and role	Description
0.1	06/07/22	[REDACTED] Senior Business Analyst	Initial draft
0.2	07/02/23	[REDACTED] Senior Business Analyst	Change of scope and other details
0.3	23/03/23	[REDACTED] privacy analyst	Redrafted following internal changes project team
0.4	19/04/23	[REDACTED] privacy analyst	Updated to reflect feedback from Senior Business Analyst
0.5	26/04/23	[REDACTED] privacy analyst	Updated to reflect feedback from Principal Privacy Advisor (ISP)
0.6	27/04/23	[REDACTED] privacy analyst	Updated to reflect feedback from Product Owners
0.7	28/04/23	[REDACTED] privacy analyst	Updated to reflect feedback from partner agencies
1	03/07/23	[REDACTED] privacy analyst	Final version
1.1	05/07/23	[REDACTED] privacy analyst	Updated R7 after discussions with senior management
1.2	22/08/23	[REDACTED] privacy analyst	Small editing changes – see Appendix 4

Distribution list for external distribution

Version # sent	Date sent	Recipient email address	Reason for sending
0.6	27/04/23	[REDACTED]	Feedback
0.6	27/04/23	[REDACTED]	Feedback

0.7	28/04/23	[REDACTED]	Consultation
-----	----------	------------	--------------

Disclaimer and assumptions

This PIA has been prepared by the New Zealand Customs Service - Te Mana Ārai o Aotearoa (Customs). Customs is the lead agency for the New Zealand Traveller Declaration and works closely with Ministry of Business, Innovation and Employment (MBIE) and Ministry for Primary Industries (MPI) to deliver the online system.

This PIA has been prepared to review the privacy implications of primary line web applications (Te Tomokanga) and secondary line web applications (MPI Search and MPI Roaming) as part of the New Zealand Traveller Declaration (NZTD) and whether this complies with the Privacy Act and related Information Privacy Principles.

This PIA reflects the operation of web applications used in the arrival hall as it is currently envisaged. It is intended to be a “living document” and will be regularly updated to reflect changes that arise as the NZTD is progressively rolled out and adapted to respond to changes in the broader environment.

Updating the PIA to reflect changes will be the responsibility of the product owners.

A version of this PIA will be made publicly available alongside the communication collateral deployed with the NZTD. This will support the public to understand the collection, storage, use and sharing of personal and third-party information. This is a transparency decision, intended to support public trust in the operation of the NZTD.

Glossary

Abbreviation	Meaning
Alert	A recording within the CusMod system that a particular person or goods are of interest to Customs or an external agency that is authorised to use this facility.
ANA	Advance Notice of Arrival The person in charge of a craft that is en-route to New Zealand (from a point outside New Zealand) must, within the prescribed time, provide Customs with an advance notice of arrival, unless otherwise approved by the chief executive.
API	Advance Passenger Information For security reasons, most countries require airlines to provide details about their passengers before they travel. This is known as Advance Passenger Information (API).
APP	Advance Passenger Processing If notified of the requirement to do so, airlines must provide Advance Passenger Processing information to the Chief Executive of MBIE

	(Immigration NZ) about every passenger and crew member on their flights coming to or leaving New Zealand.
BDF	New Zealand Traveller Declaration - Border Decision Framework A framework that sets in motion a risk assessment of travellers to New Zealand. BDF is an assessment of a traveller declaration against rules; it does not do the actual risk assessing itself.
Biometric information	Biometric information, in relation to a person, means information that comprises— (a) 1 or more of the following kinds of personal information: (i) a photograph of all or any part of the person’s head and shoulders; (ii) impressions of the person’s fingerprints; (iii) a scan of the person’s irises; and (b) an electronic record of the personal information that is capable of being used for biometric matching
Border agencies	The border agencies are New Zealand Customs Service, Ministry for Primary Industries for Biosecurity New Zealand, and the Ministry of Business, Innovation and Employment for Immigration New Zealand.
Category of information	Section 304 of the Customs and Excise Act 2018 defines two categories of information in regards to disclosures: <i>Category 1 information</i> means any information held by Customs,— a) including information relating to— (i) persons; (ii) goods; (iii) craft; but b) excluding Category 2 information <i>Category 2 information</i> means— a) the following information in relation to any person: (i) arrival and departure information; (ii) biometric information; (iii) passenger name record information; and b) intelligence assessments and reports generated by Customs Section 41A of the Biosecurity Act refers to the following definition of border information: border information— (a) means information— (i) that is required to be supplied to the Ministry or the Customs by or under this Act or the Customs and Excise Act 2018, or both, for a border protection purpose; or

	<p>(ii) that is otherwise lawfully supplied or collected for a border protection purpose; and</p> <p>(b) includes, without limitation, information about—</p> <p>(i) goods, persons, or craft:</p> <p>(ii) import or export transactions:</p> <p>(iii) importers or exporters; and</p> <p>(c) also includes data or information that is derived from, or related to, any information referred to in paragraphs (a) and (b) or any analysis of that information</p>
COLIN	COLIN is the Customs mobility app that allows frontline Customs Officers to remotely record activities of interactions. Users can add photos of the interaction, capture tools used, officers present, and the outcome of the interaction.
Customs	New Zealand Customs Service - Te Mana Ārai Aotearoa
CusMod	Customs' primary system for border management that records every movement of passengers, goods and craft across New Zealand's border. CusMod processes advanced passenger, goods and craft information to facilitate legitimate trade and travel.
DIA	Department of Internal Affairs - Te Tari Taiwhenua
DOB	Date of birth
High Risk Control Point HRCP	The High Risk Control Point in the Biosecurity area is used by MPI Biosecurity Officers to process travellers who do not qualify to pass through the Low Risk Control Point.
INZ	Immigration New Zealand, a part of the Ministry of Business, Innovation, and Employment
InterPol	The International Criminal Police Organisation An international organization that facilitates worldwide police cooperation and crime control.
IPP	Information privacy principle under section 22 of the Privacy Act
Low Risk Control Point LRCP	The Low Risk Control Point is at the entry to the biosecurity area in arrival ports in New Zealand. This control point will allow travellers who have been automatically assessed as low risk (across all agencies) to bypass some of the biosecurity controls.
MBIE	Ministry of Business, Innovation and Employment - Hīkina Whakatutuki
MoH	Ministry of Health – Manatū Hauora

MPI	Ministry for Primary Industries – Manatū Ahu Matua
MRZ Scanner	Machine Readable Zone Scanner A mobile device that can scan passports, ID cards, visas and other documents that have a machine-readable zone.
NZeTA	New Zealand Electronic Travel Authority
NZTD	New Zealand Traveller Declaration
Personal information	Personal information (a) means information about an identifiable individual; and (b) includes information relating to a death that is maintained by the Registrar-General under the Births, Deaths, Marriages, and Relationships Registration Act 1995 or any former Act (as defined in section 2 of the Births, Deaths, Marriages, and Relationships Registration Act 1995)
PIA	Privacy Impact Assessment A tool used by agencies to help identify and assess the privacy risks arising from the collection, use or handling of personal information. A PIA will also evaluate ways to reduce privacy risks.
PNR	Passenger Name Record – generated at the time of the booking and consists of the passenger's personal and journey details.
Pre-travel manifest	A manifest is a document listing the cargo, passengers, and crew of a ship, or aircraft for the use of customs and other officials. Where such a list is limited to identifying passengers, it is a passenger manifest or passenger list.
Primary line	The primary line is the point in the arrivals hall where the traveller presents their passport to either an officer at the booth or an eGate. This is also the point where an application for a visa and/or entry permission may be made.
Privacy Act	Privacy Act 2020
Secondary Line	A place where travellers may be directed for further interaction with a border officer because an assessing officer considers further questioning or an inspection is required.
Te Tomokanga	Te Tomokanga means the entrance hall in te reo Māori.
Third-party information	Information collected by an entity that does not have a direct relationship with the user the data is being collected from.
TJI	New Zealand Traveller Declaration - Traveller Journey Index The TJI is a centralised data orchestration system. The TJI records references to data stored in their proprietary systems. It captures the

	references for a unique journey record for a single journey made by a traveller. It is the core system component that assesses and authorises other parts of NZTD to risk assess the traveller upon reaching New Zealand, prior to being processed at the Primary Line. TJI does not process any data itself.
Traveller Crossing record	The amalgamation of the TJI record and any interactions that happened with the traveller at the airport as part of that particular journey.
UI	User Interface

1. Introduction and purpose

This PIA will assess the following NZTD's *Port Operations Systems* used in the arrival hall at airports:

- *Primary Line web applications - Te Tomokanga primary, Te Tomokanga Low Risk Control Point and Te Tomokanga High Risk Control Point; and*
- *Secondary Line web applications - MPI search and MPI roaming*

The PIA will assess whether these systems comply with the Privacy Act and related Information Privacy Principles (IPPs). It explains the process followed, the factors considered and the steps that will be taken to ensure the privacy of travellers to New Zealand will not be adversely affected by the use of these port operations systems.

The New Zealand Traveller Declaration (NZTD) is an online system for travellers to complete a declaration before they enter New Zealand and answer questions for Customs, Immigration and Biosecurity¹². The NZTD will be an alternative to the paper-based passenger arrival card.

The aim is to modernise the border, help passengers move through airports more efficiently, and improve the safety and security of New Zealand by being able to assess passenger information earlier in their journey. This will support increased compliance among passengers and the ability to identify non-compliant passengers earlier.

It is estimated that by 2025, more than 18 million travellers will have used NZTD across air and maritime ports.

Initiative overview

Context

Port operations systems are the systems associated with processing travellers at air and maritime ports. The vast majority (>80%) of travellers crossing the border do so at one of the 5 international airports, with the remainder crossing at maritime ports or small airports. The 5 international airports all have permanent infrastructure in place to support border operations for Biosecurity, Customs and Immigration purposes. The permanent infrastructure at the international airports includes

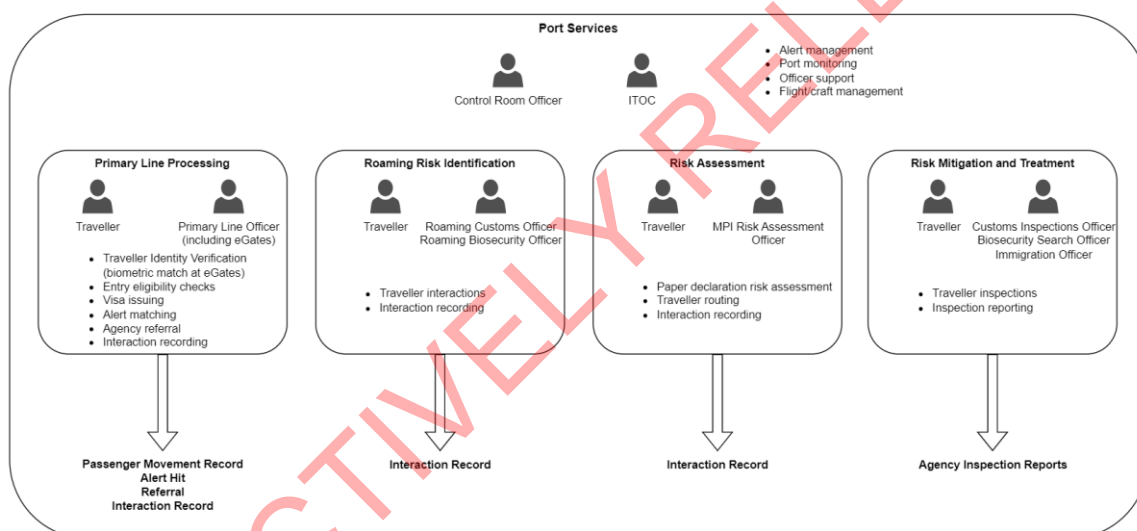
¹ There are currently no Ministry of Health requirements active in NZTD but the processes and systems have been established to enable the management of health requirements at the border to minimise health risks as we saw during the COVID-19 pandemic.

² The arrival card serves multiple purposes for multiple border agencies. For more information, please refer to the PIA on the Digital Traveller Declaration.

eGates, primary line booths, control rooms, IT infrastructure, search areas, fixed x-rays and office space for staff.

Processing travellers involves, among other things:

- Identity matching and verification.
- Checking eligibility and entitlement to enter New Zealand.
- Making a decision on whether to grant a visa on arrival to a traveller.
- Making a decision on whether a traveller is granted permission to enter New Zealand.
- Creating a border crossing record (Passenger Movement).
- Checking traveller details against Alert lists.
- Performing referrals based on traveller risk assessments and/or information provided by a traveller.
- Recording interactions with travellers for NZTD purposes.
- Performing risk mitigations through traveller interviews and inspections.
- Undertaking flight/craft management activities like opening, balancing and closing movements.³



Primary line processing

Processing a traveller involves several steps.

Step 1 – Identity verification

A key step in the primary line processing is the identification of the traveller to verify they are who they claim to be. This involves analysis of the traveller against their travel documents (usually a passport) and normally includes a face-to-passport match by a human border officer, or an automated biometric check against the image on an ePassport when a traveller presents to an eGate. This step provides a very high level of confidence in terms of who is attempting to enter New Zealand and the quality of information in the resulting passenger movement records.

³ Administrative tasks include opening and closing flight / craft movements, balancing passenger/crew numbers against Advanced Passenger Information and Advanced Notice of Arrival data and arrival card processing (physical card sorting, scanning and storing).

Step 2 – Retrieving a NZTD

A passport scan using the existing document readers at the booth at the Primary Line or by swiping the passport using a MRZ device at the High Risk Control Point or at the MPI Secondary Line will be needed to query the Traveller Journey Index⁴ to retrieve a matching NZTD. In case there is no response from the passport readers, the border officer will manually enter the same details in an UI in order to retrieve a matching NZTD record.

Step 3 – NZTD checking

As the traveller declaration/ paper-based passenger arrival card is a requirement to cross the border, a process has been put in place to verify that:

- a traveller declaration has been submitted,
- the traveller declaration requirements have been met,
- the traveller declaration belongs to the traveller who is presenting it at the primary line.

This will allow the primary line to direct and refer travellers based on information provided in their traveller declaration and to provide instructions to travellers who are yet to complete a traveller declaration.

Step 4 – entry eligibility checks

All travellers arriving in New Zealand must be eligible to enter New Zealand through one or more methods. Travellers must either be:

- New Zealand citizen
- New Zealand resident visa holder
- The holder of another type of valid visa to New Zealand
- The holder of a valid New Zealand Electronic Travel Authority (NZeTA) if their nationality is a visa waiver country.
- A citizen of a country where visas can be issued on arrival into New Zealand.

Primary line processing must confirm that at least one of these requirements has been met prior to allowing a traveller to enter New Zealand. If not, travellers are referred to INZ.

Step 5 -Visa issuing

Some entry classes for non-New Zealand citizens involves the issuing of a visa upon arrival. This is offered to citizens of visa waiver countries or if you hold a current Australian permanent resident visa. If a traveller presents a passport from one of these countries at the primary line, the AMS system by INZ will issue this visa as a result of the passenger movement record being sent to INZ.

Step 6 - Alert Matching

Traveller details are checked against alert holdings at the primary line. Biographic and travel document details are checked and matched if the traveller is of interest to a New Zealand government agency or InterPol.

⁴ Please refer to PIA Traveller Journey Index.

Step 7 - Alert Hits

When a traveller matches one or more alerts, an 'alert hit' is created. Details of the reason for alert and the required actions will then be provided to the primary line officer for execution. Notifications may also be sent to the Control Room so the traveller can be monitored as they proceed through the port. Alert hits also trigger activity reports to be generated in CusMod for Inspection Reporting purposes and subsequent jobs being placed on teamwork queues depending on which agency the alert is for and the required action that needs to be taken.

Step 8 - Passenger movement record

Once all of the above checks have completed, a passenger movement record will be created by the primary line to capture the official border crossing of the traveller. CusMod is the system of record for the passenger movement and this passenger movement will be send to INZ.

Step 9 - Interaction recording

Interactions that take place between a border officer and a traveller, including as part of primary line processing, will be recorded in line with operational processes. These interactions are known as 'referrals' and they generally relate to concerns with the traveller's behaviour, appearance and/or comments made to an officer. These interactions capture details from the officer in terms of the concern and the recommended action to be taken by the operational agencies at the port. This will result in subsequent secondary interventions for the traveller

Roaming risk identification

Customs and MPI Biosecurity officers will often monitor activities in the port to ensure risks are identified for appropriate treatment. These officers will need access to traveller declarations to see what a traveller has or has not declared. They will also need to be able to view any prior interactions this traveller has had on this journey and record new interactions. This will be explained in more detail in the table below.

Traveller routing

All travellers who require further interaction with a border agency will need to be routed to the appropriate agency(s) prior to leaving the controlled area at the port. Travellers should be able to self-select where to go with controls in place on the exit pathway to make sure all travellers who require further interactions are identified and captured. Travellers may require further interaction because of the risk assessment of their traveller declaration, they may be subject of an alert, or they may have had an interaction with a border officer where the recommended action is for subsequent follow up. Key locations for traveller routing are the Low Risk Control Point and MPI Risk Assessment station both in the Biosecurity space.

Risk mitigation

Any traveller requiring further interaction with an agency will typically involve interviewing and person/baggage searches. These activities take place in designated search areas at the 5 international airports. Travellers may have further interactions with more than one agency depending upon what risks have been identified in the risk assessment process.

Te Tomokanga

The following primary line web applications and secondary line web applications will be used to process travellers on arrival and will be the focus of this PIA. Appendix 1 shows the different steps for processing a passenger within Te Tomokanga and Appendix 2 for MPI Search.

<p>Te Tomokanga at the primary line</p>	<p>Te Tomokanga will be used by Customs officers to process traveller declarations at the booth at the Primary line. This user interface will allow for the traveller declaration status to be confirmed, to clear referrals if the Customs officer decides a secondary assessment is not required, and any interaction records to be captured.</p> <p>This process will involve a border officer scanning a traveller's passport which will trigger a search on Traveller Crossing records based on the passport data. The Customs officer can record interactions and make decisions regarding the need for referral to the other border agencies for secondary processing.</p> <p>The devices used will be Customs domain joined desktops with passport readers. This will not be a change to what is currently being used.</p>
<p>Te Tomokanga Low Risk Control Point</p>	<p>The Low Risk Control Point will be at the entry to the biosecurity area in arrival ports in New Zealand. This control will allow travellers who have been automatically assessed as low risk (across all agencies) to bypass some of the biosecurity controls (MPI Risk Assessment) resulting in an improved experience for the traveller.</p> <p>This control point is delivered as a "Digitally enabled human" where a border officer will scan a traveller's passport into a system where the traveller's eligibility to use the low risk control point is returned on the screen. The intention is for this interaction to be very rapid. This interaction will automatically be captured in the Te Tomokanga system.</p> <p>The devices that will be used is a Customs or MPI laptop with a passport reader.</p>
<p>Te Tomokanga High Risk Control Point</p>	<p>The High Risk Control Point in the biosecurity area will be used by MPI Biosecurity Officers to process travellers who do not qualify to pass through the Low Risk Control Point.</p> <p>This user interface will allow for the traveller declaration status to be confirmed, to clear referrals if the MPI officer decides a secondary assessment is not required, and any interaction records to be captured.</p> <p>This web-based user interface will be deployed on a dedicated device for this single purpose. This interaction will involve a MPI Biosecurity officer scanning travellers' passports which will trigger a search on Traveller Crossing records based on the passport data. It then enables the MPI Biosecurity officer to assess the traveller and add interactions to the traveller crossing record associated with the traveller.</p> <p>The devices that will be used will be laptops with a MRZ scanner to read passports.</p>

MPI search	<p>The MPI Search user interface in the Biosecurity area will be used by MPI Biosecurity officers to view traveller declarations, referrals and interactions for those travellers who require biosecurity risk treatment.</p> <p>This user interface will allow MPI Biosecurity officers to view all details of the traveller declaration, directives from risk assessment, previous interactions and any interaction records to be captured.</p> <p>This interaction will involve a Biosecurity Officer scanning traveller passports which will trigger a search on Traveller Crossing records based on the passport data. The information returned to the user will be a complete set and allow for a fully detailed interaction to take place.</p> <p>This web-based user interface will be deployed on a dedicated device for this single purpose. The devices that will be used will be laptops with a MRZ scanner to read passports.</p>
MPI roaming	<p>The MPI Roaming App is a Single Page App (SPA)⁵, accessed on mobile devices used by MPI Roaming Officers to aid risk assessment by allowing them to view a traveller declaration, interactions, and referrals when they are roaming the airport and interacting with travellers outside of the set MPI points. Additionally, they will be able to capture interactions and referrals, and will be able to clear the referrals if the MPI officer decides a secondary assessment is not required.</p> <p>The devices used will be an Android or iPhone. The MPI Roaming App will be web based to allow this.</p>

Issues this project will address:

The introduction of the digital traveller declaration requires a number of new port operations services. Traveller declaration checking will need to be delivered in a fully integrated manner at the primary line and in the customs and biosecurity space. Access to the information collected by the traveller declarations that biosecurity officers and customs officers are legally authorised to see will need to be provided⁶. Roaming officers will also need to be able to view traveller declarations and to be able to capture interaction records against a traveller. The low risk control point and MPI risk assessment stations will need to be able to identify all travellers who require secondary agency intervention due to something they have digitally declared, any alerts or as a result of any interaction records.

Benefits it will bring to border agencies:

- A more efficient operational process for border officers upon arrival.
- Less risk to New Zealand’s border⁷.

⁵ A Single Page Application is a web application that is designed to be displayed as a single, static page.

⁶ AIMS, an MBIE platform, will allow for access to traveller declarations for immigration officers processing traveller immigration referrals.

⁷ Border agencies work together to protect New Zealand by reducing risks from people, goods or craft arriving at the border.

Benefits to others:

- A more efficient process for travellers.

Key privacy lessons learned from NZTD Trials

Before go-live, there have been several trials of NZTD processes. These trials tested NZTD systems, processes and functionality and provided an opportunity for border staff training.

Here are some examples of the privacy lessons learned for the primary and secondary line web applications:

- Privacy screens fell off computer screens.
- Privacy screens do not allow for touch screen usability.
- As free text was not ideal at the HRCP, buttons have been put in place to improve efficiency.

2. PIA scope

This PIA will focus on the privacy impact of the primary line web applications (Te Tomokanga) and secondary line web applications (MPI Search and MPI Roaming).

This PIA will not cover:

- The privacy impact of the broader NZTD programme, incl. the choice of strategic direction of the NZTD, the policy analysis or legislative settings that reflect that direction.
- The privacy impact of current border operations incl. the risk-based selection of passengers and goods for intervention or the search processes undertaken during an intervention.
- The privacy impact of the existing processing system CusMod.
- The privacy impact of the Inspection Reports, Activity Reports and the existing processes around these.
- The privacy impact of the existing COLIN web and mobile app.
- The privacy impact of the existing Traveller Crossing report.
- The privacy impact of INZ's platform AIMS.
- The privacy impact of the Traveller Journey Index⁸.
- The privacy impact of the Digital Traveller Declaration⁹.
- The privacy impact of the Border Decisions Framework¹⁰.
- The privacy practices of the participating agencies, e.g. MPI and INZ.

3. Executive risk summary

A risk-based approach to the use of primary line web applications (Te Tomokanga) and secondary line web applications (MPI Search and MPI Roaming) is being taken. We believe that these web

⁸ Please refer to PIA Traveller Journey Index.

⁹ Please refer to PIA Digital Traveller Declaration.

¹⁰ Please refer to PIA Border Decisions Framework.

applications best meet our needs, in the most cost-effective way, while providing adequate privacy and security protections.

The following residual risks have been identified. Controls have been put in place or are still under development. A detailed description of risks and controls can be found in Appendix 3, Project Risks and Controls table.

		Consequence				
		Insignificant	Minor	Moderate	Major	Severe
Likelihood	Certain		R7			
	Likely					
	Possible					
	Unlikely	R2	R1, R4, R5, R6			
	Rare					

* R3 - Risks in regard to IPP 5 - Storage and security of personal information - The NZTD cyber security team assessed the security risks for these primary and secondary line web applications and is responsible for the Certification & Accreditation (C&A) process and security risk assessment. For more information on security risks, please refer to the security C&A.

4. Openness and transparency

IPP 3 of the Privacy Act requires agencies to be open and transparent about the way they manage personal information. To meet these openness and transparency obligations, we will:

- Make this PIA public.
- Have a NZTD privacy statement (<https://www.travellerdeclaration.govt.nz/privacy>) that will explain how the border agencies will collect, use and disclose personal information travellers will provide through the NZTD online form.
- Engage where required and appropriate with anyone who has particular concerns with the use of the Primary and Secondary Line Web Applications.
- Have a dedicated website for NZTD - <https://www.travellerdeclaration.govt.nz/>

5. Personal information to be captured

The following personal information will be captured by the primary line web applications (Te Tomokanga) and secondary line web applications (MPI Search and MPI Roaming). This information will be captured by a border officer scanning a traveller's passport or by manually entering the passport details.

Personal information from passengers:

- Passport number
- Name

- Nationality
- Date of birth

Personal information from processing officers:

- Usernames of processing officers (Customs, MPI)

6. Assessment of privacy impacts

This section advises on the privacy impacts of NZTD's primary line web applications (Te Tomokanga) and secondary line web applications (MPI Search and MPI Roaming) in consideration of the IPPs of the Privacy Act.

6.1 Collection of personal information

IPP 1 - Purpose of collection of PI
<p>Personal information shall not be collected by any agency unless:</p> <ul style="list-style-type: none"> • the information is collected for a lawful purpose connected with a function or activity of the agency; and • the collection of that information is necessary for that purpose. <p><i>Information sought should be necessary for the purpose of your project. It is not enough for the information to be merely helpful or nice to have.</i></p>

1. *Describe how collection matches the functions or activities of the border agencies. If there are other agencies involved as the collecting agency, describe how their purposes are met.*

In order to retrieve the traveller's digital declaration, the traveller will have their passport scanned via CusMod on arrival. Personal information that will be captured is surname, DOB, nationality and passport number.

Interaction record - relating to concerns with the traveller's behaviour, appearance and/or comments made to a border officer- capture details from the border officer in terms of the concern and the recommended action to be taken by the operational agencies at the port.

2. *Describe how collection is necessary for those purposes.*

Capturing personal information (name, passport number, nationality and DOB) is necessary for identity verification services. Without this information, it would not be possible to accurately identify a traveller and retrieve their digital traveller declaration.

Collection of primary and secondary Processing Officers' usernames is a crucial component of a comprehensive audit trail of any actions performed by said user (scanning a passport, inputting passport details, searching for a traveller declaration, any traveller declarations that were successfully retrieved).

The collection of personal information by the primary and secondary web applications supports the regulatory delivery of border control services.

3. *State any risks.*

There is a risk of overcollection by border officers including unnecessary information in the interaction records.

4. *State any policies / processes that exist, or may need to be developed, to achieve or maintain consistency with IPP 1 or to mitigate risks.*

- Role-based training to ensure the border officers understand the scope of the lawful authority and lawful purpose for collecting the personal information and what personal information is necessary to fulfil this.
- Standard operating procedures will provide the border officers with information and guidance on the required processes and procedures.
- Education programmes to ensure border officers understand the expectations and responsibilities that apply to them.

IPP 2 – Source of personal information

IPP 2 of the Privacy Act requires that an agency shall collect information directly from the individual concerned, unless an exception applies. Broadly, the exceptions under IPP2(2) are:

- (a) that non-compliance would not prejudice the interests of the individual concerned;
- (b) that compliance would prejudice the purposes of the collection;
- (c) that the individual concerned authorises collection of the information from someone else;
- (d) that the information is publicly available;
- (e) that non-compliance is necessary to avoid prejudice to maintenance of the law, for the enforcement of a pecuniary penalty law, for the protection of public revenue, for the conduct of court or tribunal proceedings, or to prevent or lessen a serious threat to the life or health of an individual; or
- (f) that compliance is not reasonably practicable in the circumstances of the particular case.
- (g) that the information will not be used in a form in which the individual concerned is identified or will be used for statistical/research purposes and not published in a form that could reasonably be expected to identify the individual concerned.

5. *Describe whether information will be collected directly from the individual.*

Personal information will be collected directly from the individual, by scanning the passport that the passenger supplies or by manually entering the passport details by the processing officer.

The information in the digital traveller declaration is also collected directly from the traveller (or in case of a third party filling out the digital traveller declaration on their behalf) when they complete their digital traveller declaration. For more information on this, please refer to the PIA Digital Traveller Declaration.

The username of the primary processing officer and MPI secondary officer is logged as the username used to login to the machine.

6. *Describe whether an exception applies etc.*

n/a

7. *State any risks.*

n/a

8. *State any policies / processes that may need to be developed to achieve or maintain consistency and/or mitigate risks.*

n/a

IPP 3 – Collection of information from subject

IPP 3(1) of the Privacy Act requires that where an agency collects personal information directly from the individual concerned, the agency shall take reasonable steps to ensure that the individual knows:

- (a) the information is being collected;
- (b) the purpose of collection;
- (c) all intended recipients of the information;
- (d) name and address of the agency collecting the information and name and address of the agency holding the information;
- (e) whether collection is authorised or required by law – and the particular law, and whether it is mandatory or voluntary for the individual to supply the information;
- (f) consequences of not providing the information; and
- (g) their rights of access to (IPP6) and rights to correction (IPP7) of the personal information.

Under IPP 3(2) this should be done prior to collection, or as soon as practicable after collection.

Under IPP 3(3), agencies can forego notification of (a) to (g) above if the agency has recently communicated the same information to that individual in relation to collecting the same (or same type of) personal information from that individual. Please see the other exceptions under IPP 3(4), broadly:

- (a) that non-compliance would not prejudice the interests of the individual concerned;
- (b) that non-compliance is necessary to avoid prejudice to maintenance of the law, for the enforcement of a law imposing a pecuniary penalty, for the protection of public revenue, for the conduct of court or tribunal proceedings, or to prevent or lessen a serious threat to the life or health of an individual;
- (c) that compliance would prejudice the purposes of the collection;
- (d) that compliance is not reasonably practicable in the circumstances of the particular case; or
- (e) that the information will not be used in a form in which the individual concerned is identified or will be used for statistical/research purposes and not published in a form that could reasonably be expected to identify the individual concerned.

9. Describe how individuals will be notified of **all** the required information outlined in IPP3. Describe how individuals will be informed about the complete set of information to be collected.

The NZTD privacy statement will explain how border agencies will collect, use and disclose personal information travellers will provide through the NZTD online form. Travellers are asked to confirm they have understood how their information is being used before they fill out their traveller declaration. The privacy statement is also available on the dedicated website for NZTD (<https://www.travellerdeclaration.govt.nz/privacy>).

Section 4 of this PIA provides more information on how NZTD will meet its openness and transparency obligations.

10. Describe any exceptions.
n/a

11. State any risks (eg, only being able to advise on some of these elements, when there are no exceptions).

If travellers do not read the privacy policy, they could be unaware what the digital traveller declaration will be used for and which agencies will have access to the information.

12. State any policies / processes that may need to be developed to achieve or maintain consistency and mitigate risks.

Travellers will have to accept the privacy statement indicating they have read and understood the privacy policy before submitting their digital traveller declaration.

In the case of a third party filling out the traveller declaration on behalf of the traveller, this nominated delegate will be responsible for ensuring that the traveller understands their privacy rights.

IPP 4 – Manner of collection

Under IPP 4(1) Personal information shall only be collected by an agency

- (a) by lawful means; and
- (b) in the circumstances of this project, are by means that are
 - (i) fair, and
 - (ii) do not intrude unreasonably on the personal affairs of the individual concerned.

Particular care should be taken with regard to collection of personal information from children or young persons.

13. Describe whether the collection is lawful, fair and not unreasonably intrusive (note - if an element is not met, it will be a risk).

The border agencies have the legal authority to collect personal information for the purpose of border management.

Having to show your passport when visiting a country is common practice, explicitly provided for in New Zealand legislation and not perceived as unreasonably intrusive.

14. State any risks (eg, if non-provision of information will result in the individual being unable to access the services – explain why this is not unfair in the circumstances).

n/a

15. State any policies / processes that may need to be developed to achieve or maintain consistency / mitigate risks.

n/a

6.2 Storage and security

IPP 5 – Storage and security of personal information
<p>IPP 5(a) An agency holding personal information must ensure that information is protected by such security safeguards as are reasonable in the circumstances, against:</p> <ul style="list-style-type: none">• loss;• unauthorised access, use, modification or disclosure; and• other misuse. <p>IPP 5(b) This is also required when the information is transferred to a third party.</p>

16. Describe security compliance including the security safeguards that will be in place.

Only authorised users of the Te Tomokanga, MPI Search and MPI Roaming applications have access to view the travellers' personal information.

The computers used by border officers to access the port operations systems will have computer privacy screen filters. A privacy screen is a thin layer of polarised plastic that significantly reduces the viewing angle of the screen, reducing the chance of visual hacking.

The MPI roaming device will have a camera. This will not be used by officers to take pictures but purely to scan passports for the retrieval of the digital traveller declaration.

All Te Tomokanga devices (laptops, phones, MRZ scanners) will be passcode protected.

The NZTD cyber security team followed a 'secure by design' approach for NZTD, complemented by engaging an independent external third party to perform and complete penetration testing and configuration reviews. Particular focus was given to the use of API's given their widespread use within NZTD, and the increasing sophistication of attacks by malicious threat actors against this vector.

There are current organisational, procedural and technical safeguards in the Customs/ airport environment.

17. Describe how these are reasonable in the circumstances.

These controls are considered best practice.

18. State any risks here (eg, 3rd party access, unsecured information etc).

The NZTD cyber security team assessed the security risks for these primary and secondary line web applications and is responsible for the Certification & Accreditation (C&A) process

and security risk assessment. For more information on security risks, please refer to the security C&A.

19. *State any policies / processes that may need to be developed to achieve or maintain consistency and/or mitigate risks.*

See previous comment.

20. *If a 3rd party platform is to be used, what:*

[REDACTED]

6.3 Access, correction and accuracy

IPP 6 – Access to personal information
<p>Where an agency holds personal information, the individual concerned shall be entitled</p> <ul style="list-style-type: none">• IPP 6(1)(a) to obtain confirmation of whether the agency holds personal information about them; and• IPP 6(1)(b) to have access to their personal information. <p>Under IPP 6(2), if an individual is given access to their personal information, they must be advised that, under IPP 7, they may request correction of that information.</p> <p>Under IPP 6(3), IPP 6 is subject to Part 4 (Access to and correction of personal information) of the Privacy Act.</p>

21. *Describe compliance elements – for example, can Customs (and other relevant agency) confirm the information exists and is held by Customs? Can Customs provide that information in a form requested by the individual concerned? How will the individual be advised of their right to request correction of the information?*

The primary web applications Te Tomokanga and the secondary web applications (MPI search and MPI roaming) only collect personal information (by scanning a passport or manual entry) to retrieve the traveller's digital traveller declaration. If the traveller wishes to submit an information request to receive the NZTD data held on them, they can do so by contacting the contact centre¹¹. This is covered in the privacy statement that travellers will need to accept before submitting their digital traveller declaration. The privacy statement is also available on the dedicated website for NZTD.

Each agency has processes for managing access requests in place and a process for managing requests which cover information held by multiple agencies will be agreed and led by Customs.

22. *State any risks. (Note that IPP6 creates legally enforceable rights for the individual concerned).*
n/a

¹¹ For more information about the right to access, please refer to the PIA Whare Āwhina.

23. *State any policies / processes that may need to be developed to achieve or maintain consistency and/or mitigate risks.*

n/a

IPP 7 – Correction of personal information

Under IPP 7(1), where an agency holds personal information, the individual concerned is entitled to request correction of that information.

Under IPP 7(2), the agency must then take such steps that are reasonably in the circumstances (considering the lawful purpose of use of the information) to ensure that the information is accurate, up to date, complete and not misleading.

Under IPP 7(2A), when making this request or at any later time, the individual may also provide the agency with a statement of the correction sought (**Statement of Correction**) and request that the Statement of Correction is attached to the information if the agency does not make the correction.

Under IPP 7(2B), where the agency is not willing to correct the information following a correction request, the agency must take reasonable steps to attach the Statement of Correction provided by the individual so that it will always be read alongside the information.

Under IPP 7(3), where the agency has corrected the information, or attached a Statement of Correction to the information, the agency must (if reasonably practicable) inform each person or agency to whom the information has been disclosed of those steps taken.

24. *Description of compliance – for example, can Customs correct that information? Can Customs **attach** a statement that the correction was sought, to the personal information itself? Can Customs inform the third parties it has disclosed the personal information to?*

The personal information the primary and secondary line web applications collect is collected directly from the traveller by scanning a traveller's passport. Rights to correction should be unnecessary. However, the right to correction for the information collected by the NZTD is covered in the privacy statement that travellers will need to read and accept before submitting their digital traveller declaration.¹²

25. *Description of compliance – if relevant, will 3rd party recipients (eg other agencies) be able to be advised?*

n/a

26. *State any risks.*

n/a

27. *State any policies / processes that may need to be developed to achieve or maintain consistency and/or mitigate risks.*

n/a

¹² For more information about the right to correction, please refer to the PIA Whare Āwhina.

IPP 8 – Accuracy of personal information to be checked before use

An agency that holds personal information shall not use or disclose that information without taking steps that are (in the circumstances) reasonable to ensure that the information is accurate, up to date, complete, relevant and not misleading. These steps should be taken having regard to the purpose for which the information will be used (IPP1).

28. *Describe compliance with information accuracy – for example, will collection support accuracy? Will steps be taken to maintain accuracy over the project / information’s lifespan? Are these reasonable steps in the circumstances or could more be done?*

Identity verification processes at the Primary line (passport control) will ensure the person providing the personal information is identified as the individual. The chances of any inaccuracies here would be nil.

The PIA Traveller Journey Index provides more information on data matching rules and the risk of pulling up the incorrect digital traveller declaration is being minimalised.

29. *Describe how these steps are consistent with the purpose of collection/use under IPP1.*

The NZTD enables border agencies to collect personal information directly from travellers for the purpose of managing border requirements. The information will be collected directly from the individual by scanning the traveller’s passport and retrieving their digital traveller declaration.

30. *State any risks.*
n/a

31. *State any policies / processes that may need to be developed to achieve or maintain consistency and/or mitigate risks.*
n/a

6.4 Retention, use and disclosure

IPP 9 – Agency not to keep personal information for longer than necessary

An agency that holds personal information shall not keep that information for longer than is required for the purposes for which it may lawfully be used.

32. *Describe term of data retention - how long it is required to meet the lawful use under IPP 1.*

The traveller record will need to be maintained for a minimum period for operational and legal purposes, then it will be deleted following the NZTD data retention policy¹³.

Only a single journey made by a traveller will be captured. Journeys will not be joined over time and no historical database of an individual’s movements that can be used directly as an intelligence holding will be created by NZTD.

¹³ Disposal authority for NZTD is TBC.

33. *State any risks here.*

Keeping personal information longer than necessary may increase the risk of unauthorised and inappropriate access, use or disclosure and non-compliance with the Privacy Act, other laws and/or NZTD policies.

34. *State any policies / processes that may need to be developed to achieve or maintain consistency and/or mitigate risks.*

Once personal information is no longer required to satisfy legal and operational requirements, it will be completely deleted from the port operations systems.

Independent reviews and audits will ensure that the processes for the retention and deletion of personal information are adequate and operating satisfactorily.

IPP 10 – Limits on use of personal information

Personal information obtained in connection with one purpose, shall not be used for any other purpose unless the agency reasonably believes an exception applies. Exceptions are set out at IPP10(1), which broadly states:

- (a) that the purpose of use is directly related to the purpose of collection;
- (b) that the information will not be used in a form in which the individual concerned is identified or will be used for statistical/research purposes and not published in a form that could reasonably be expected to identify the individual concerned;
- (c) that the use for that other purpose is authorised by the individual concerned;
- (d) that the source is a publicly available publication, and it would not be unfair to use the information in the circumstances;
- (e) that the use for that other purpose is necessary to avoid prejudice to maintenance of the law, for the enforcement of a law imposing a pecuniary penalty, for the protection of public revenue, or for the conduct of court or tribunal proceedings; or
- (f) that the use for that other purpose is necessary to prevent or lessen a serious threat to public health or safety, or the life or health of any individual.

35. *Describe how use is consistent with collection purpose.*

The purpose of collection of the passport number, surname, nationality and DOB is to verify the traveller's identity. Information use is consistent with collection purpose as the Primary and Secondary line applications will use the information to help confirm and retrieve the passenger's matching traveller declaration when their passport is scanned. If a matching digital traveller declaration cannot automatically be retrieved on the basis of the passport scan, the border officers may perform a manual search, which if successful, will also display these details for officers to verify that the digital traveller declaration belongs to the passenger.

The personal information that will be collected will only be used for the purposes of border management.

Agencies will only have access to the data they are legally authorised to access, e.g. Customs will only have access to relevant customs data, INZ will only have access to relevant immigration data, MPI will only have access to relevant biosecurity data.

The NZTD privacy statement will explain how border agencies will collect and use the personal information travellers will provide through the NZTD online form.

36. *Describe any exceptions that may apply.*

n/a

37. *State any risks.*

- Agencies could access the data for NZTD purposes (legally authorised) but use it for a different purpose (not legally authorised) as a result of those involved having an insufficient understanding or not applying the requirements of the Privacy Act, other law and/or NZTD policies.
- Unauthorised and/or inappropriate use of a travellers' personal information provided in their digital traveller declaration by primary and secondary processing officers.
- Personal information provided by the traveller in the r declaration (both digital and paper) is subject to slightly different risk analysis processes dependent on the primary line processing pathway available to, or chosen by, the traveller.

The Primary line risk assessment of traveller declarations by an officer for Customs risk has two additional free text information fields available. There is no current corresponding analysis available for the two relevant free text fields at the primary line eGate.

A primary risk assessment, which includes information on the declaration and questioning, may result in a referral for a secondary intervention, to understand and mitigate a potential Customs risk.

38. *State any policies / processes that may need to be developed to achieve or maintain consistency and/or mitigate risks.*

- NZTD's data access policy will specify role-based access components. Requiring validation of the legal authority at both an agency and role level will provide further mitigation for this risk. For example, a Customs officer who works in border processing at the airport will have access to different information fields than an administrator of an agency's rules engine.
- Role-based training to ensure those involved understand the way in which personal information can be used, the expectations and responsibilities that apply to them and the process for managing unauthorised and inappropriate use.
- An audit trail of processing officers' actions.

- Privacy breach management processes will ensure that unauthorised and inappropriate access will be recorded, appropriately assessed, analysed and categorised, acted upon within agreed timeframes and result in improvements to privacy and security measures that will help prevent future breaches.
- Independent reviews and audits will ensure processes for dealing with unauthorised and inappropriate use are adequate and operating satisfactorily.
- Customs staff managing the eGate primary line processing pathway may exercise training and judgement to review the declaration information of a traveller and perform risk analysis equivalent to that undertaken at the primary line booth.
- Operational training and guidance for border officers should be updated to support them to exercise judgement/discretion when making these risk assessments.
- A criteria for the procurement of new eGate infrastructure is improved accessibility. It is intended that some eGates will be wider, have mobility assistance aids, and cameras at several heights. This will enable more individuals to cross the primary line using an eGate, in particular minors and individuals with mobility assistance devices. This will reduce the likelihood of this risk impacting specific groups.

IPP 11– Limits on disclosure of personal information

An agency shall not disclose personal information to any other agency or person unless the agency believes, on reasonable grounds, that:

- (a) the disclosure purpose is in connection with (or directly related to) the purpose for which the information was obtained;
- (b) the disclosure is to the individual concerned;
- (c) the disclosure is authorised by the individual concerned;
- (d) the source of the information is a publicly available publication, and in the circumstances would not be unfair;
- (e) the disclosure is necessary to avoid prejudice to the maintenance of the law by any public sector agency; for enforcing a law imposing a pecuniary penalty; for the protection of the public revenue; or for the conduct of proceedings before any court or tribunal;
- (f) the disclosure of the information is necessary to prevent or lessen a serious threat to public health, or public safety, or the life or health of an individual;
- (g) the disclosure is necessary to enable an intelligence and security agency to perform any of its functions;
- (h) the information is to be used in a form in which the individual concerned is not identified, or for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or
- (i) the disclosure is necessary to facilitate the sale or other disposition of a business as a going concern.

This principle is subject to IPP 12.

39. Describe whether information will be disclosed to any other agency or person, in what circumstances, and, if so, which exception would apply to each disclosure.

Primary Line Applications and MPI roaming and MPI search will only use the information to help confirm and retrieve the passenger's matching traveller declaration when their passport is scanned by the border agencies.

40. State any risks.

n/a

41. State any policies / processes that may need to be developed to achieve or maintain consistency and/or mitigate risks.

n/a

6.5 Offshoring of information

IPP 12 – Disclosure of personal information outside New Zealand

An agency may only disclose personal information to a foreign person or entity (recipient) in reliance on IPP11(a), (c), (e), (f), (h), or (i) if:

- (a) the individual concerned (whose personal information it is) authorises the disclosure after being informed that the recipient may not be required to protect the information in a way that, overall, is comparable to the Privacy Act;
- (b) the recipient is carrying on business in New Zealand and the agency believes the recipient is subject to the Privacy Act;
- (c) the agency believes on reasonable grounds that the recipient is subject to privacy laws that (overall) provide comparable safeguards to the Privacy Act;
- (d) the agency believes on reasonable grounds that the recipient is a participant in a prescribed binding scheme (as defined in [insert specific regulation] the Privacy Act);
- (e) the agency believes on reasonable grounds that the recipient is subject to the privacy laws of a prescribed country (as defined in [insert specific regulation]); or
- (f) the agency believes on reasonable grounds that the recipient is required to protect the information in a way that (overall) provides comparable safeguards to the Privacy Act – for example, under a contractual agreement between the agency and the recipient.

42. State personal information storage location – some of this will, necessarily, be repetition of IPP5.

[REDACTED]

43. If overseas, state whether this is a disclosure.

n/a

44. State which exceptions will be relied on for disclosing.

n/a

45. State any risks.

n/a

46. State any policies / processes that may need to be developed to achieve or maintain consistency and/or mitigate risks.

n/a

6.6 Unique identifiers

IPP 13 – Unique identifiers
Agencies shall not assign unique identifiers to individuals unless it is necessary for that agency to carry out its functions. Agencies shall not require individuals to disclose any unique identifier unless that disclosure is related to the purpose it was assigned.

47. Describe whether unique identifiers will be assigned, and whether individuals will need to disclose them.

n/a

48. State any risks.


n/a

49. State any policies / processes that may need to be developed to achieve or maintain consistency and/or mitigate risks.

n/a

7. Risk, consultation and signature

7.1 Consultation

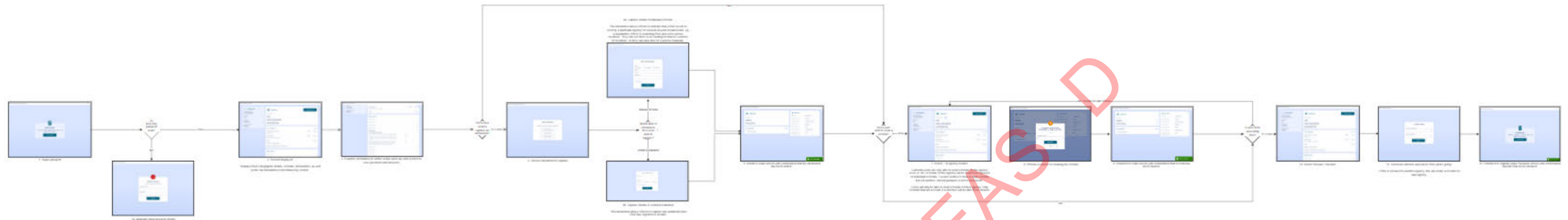
Consultation team	Team member	Date consulted	Advice given	Advice incorporated
ISP	 Principal Privacy Advisor	26 April 2023	Feedback PIA	Yes

7.2 Signatures

Name and Position	Action	Signature	Date
Principal Privacy Advisor			
Product Owner and secondary			
Central Registrar			
Product Manager			
Programme Director NZTD			

Please refer to version 1.1 for the signed version.

Appendix 2 – MPI search process flow



PROACTIVELY RELEASED

Appendix 3 – Project Risks and Controls table

Risk #	Risk rating	IPP	Reasoning	Mitigations / Controls	Residual risk
R1	low	IPP1	There is a risk of overcollection by border officers including unnecessary information in the interaction records.	<p>Role-based training to ensure the border officers understand the scope of the lawful authority and lawful purpose for collecting the personal information and what personal information is necessary to fulfil this.</p> <p>Standard operating procedures will provide the border officers with information and guidance on the required processes and procedures.</p> <p>Education programmes to ensure border officers understand the expectation and responsibilities that apply to them.</p>	Very low
		IPP2	n/a		
R2	Very low	IPP3	If travellers do not read the privacy statement, they could be unaware what the digital traveller declaration will be used for and which agencies will have access to the information.	Travellers will have to accept the privacy statement indicating they have read and understood the privacy policy before submitting their digital traveller declaration.	Very low
		IPP4	n/a		
R3		IPP5	The NZTD cyber security team assessed the security risks for these primary and secondary line web applications and is responsible for the	For more information on security risks, please refer to the security C&A.	

Risk #	Risk rating	IPP	Reasoning	Mitigations / Controls	Residual risk
			Certification & Accreditation (C&A) process and security risk assessment.		
		IPP6	n/a		
		IPP7	n/a		
		IPP8	n/a		
R4	low	IPP9	Keeping personal information longer than necessary may increase the risk of unauthorised and inappropriate access, use or disclosure and non-compliance with the Privacy Act, other laws and/or NZTD policies.	<p>Once personal information is no longer required to satisfy legal and operational requirements, it will be completely deleted from the port operations systems.</p> <p>Independent reviews and audits will ensure that the processes for the retention and deletion of personal information are adequate and operating satisfactorily.</p>	Very low
R5	low	IPP10	Agencies could access the data for NZTD purposes (legally authorised) but use it for a different purpose (not legally authorised) as a result of those involved having an insufficient understanding or not applying the requirements of the Privacy Act, other laws and/or NZTD policies.	<p>NZTD's data access policy will specify role-based access components. Requiring validation of the legal authority at both an agency and role level will provide further mitigation for this risk.</p> <p>Privacy breach management processes will ensure that unauthorised and inappropriate access will be recorded, appropriately assessed, analysed and categorised, acted upon within agreed timeframes and result in improvements to privacy and security measures that will help prevent future breaches.</p>	Very low

Risk #	Risk rating	IPP	Reasoning	Mitigations / Controls	Residual risk
				Independent reviews and audits will ensure processes for dealing with unauthorised and inappropriate use are adequate and operating satisfactorily.	
R6	<i>low</i>	IPP10	Unauthorised and/or inappropriate use of a travellers' personal information provided in their digital traveller declaration by primary and secondary processing officers.	<p>Role-based training to ensure those involved understand the way in which personal information can be used, the expectations and responsibilities that apply to them and the process for managing unauthorised and inappropriate use.</p> <p>An audit trail of processing officers' actions.</p>	<i>Very low</i>
R7	<i>Medium</i>	IPP10	<p>Personal information provided by the traveller in their declaration (both digital and paper) is subject to slightly different risk analysis processes dependent on the primary line processing pathway available to, or chosen by, the traveller.</p> <p>The Primary line risk assessment of traveller declarations by an officer for Customs risk has two additional free text information fields available. There is no current corresponding analysis available for the two relevant</p>	<p>Customs staff managing the eGate primary line processing pathway may exercise training and judgement to review the declaration information of a traveller and perform risk analysis equivalent to that undertaken at the primary line booth.</p> <p>Operational training and guidance for border officers should be updated to support them to exercise judgement/discretion when making these risk assessments.</p> <p>A criteria for the procurement of new eGate infrastructure is improved accessibility. It is intended that some eGates will be wider, have mobility assistance aids, and cameras at several heights. This will enable more individuals to cross the primary line using an eGate, in particular minors and individuals with mobility assistance devices. This will reduce the likelihood of this risk impacting specific groups.</p>	<i>Low</i>

Risk #	Risk rating	IPP	Reasoning	Mitigations / Controls	Residual risk
			<p>free text fields at the primary line eGate.</p> <p>A primary risk assessment, which includes information on the declaration and questioning, may result in a referral for a secondary intervention, to understand and mitigate a potential Customs risk.</p>		
		IPP11	n/a		
		IPP12	n/a		
		IPP13	n/a		

PROACTIVELY RELEASES

Appendix 4 – Changes since version 1.1

- Version 1.2 (August 2023)
 - Section 7.2 (signatures) removed from version 1.1
 - Appendix 4 (Changes since version 1.1) added.
 - Page numbers added.



PROACTIVELY RELEASED