

# JOINT BORDER ANALYTICS

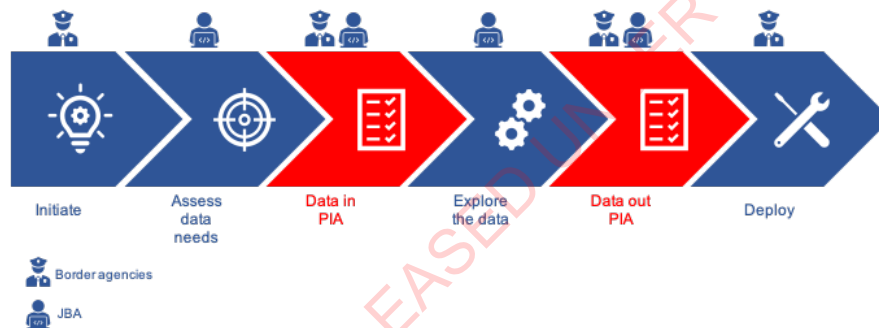
## Joint-Agency Privacy Impact Assessment Template

This PIA template should be completed for any new joint-agency analytics activity conducted by the Joint Border Analytics Centre (JBAC) on behalf of two or more border agencies. The template assists the involved border agencies to assess the lawfulness of data sharing, including data minimisation. It also assesses the lawfulness, necessity and relevance of any identifiable intelligence outputs produced as a result of the activity.

The objective of this PIA process and template is to **enable joint-agency analytics, to better deliver border enforcement functions, in a way that is open, safe, and mindful of the people behind the data.**

### Governance and accountability

Joint-agency analytics activities must be initiated by a border agency (the Lead Agency). Each involved border agency is responsible for assessing privacy or other risks raised by an activity and approving the activity. Each involved border agency must involve its privacy and/or legal team as reviewers of this PIA. JBAC can assist involved border agencies to identify or develop analytics activities and manage associated privacy risks, but JBAC cannot approve data sharing, analytics activities or outputs.



### What the PIA covers

The template relates only to activities that are managed in accordance with the Joint Border Analytics MOU and the JBAC SOPs for joint-agency activities. Thus, general privacy matters, including transparency, subject access and correction, data storage, security and JBAC access (IPPs 3, 5, 6 and 7) are addressed in the MOU and SOPs. This PIA addresses activity-level privacy matters, including data collection and disclosure, data use, accuracy and retention (IPPs 1, 2, 4, 8, 9, 10 and 11), and compliance with data analytics principles. [1]

A section 3 data sharing assessment (or 'data in' PIA) must be completed for every joint-agency activity but a section 4 output dissemination assessment (or 'data out' PIA) is only required where the output is identifiable intelligence.

### The process in brief

1. Lead Agency initiates analytics activity with JBAC
2. JBAC completes sections 1 and 2 and Appendix 1 (in consultation with involved border agencies)
3. Involved border agencies complete sections 3 and 4 as required (in consultation with JBAC)
4. JBAC completes section 5 to reflect outcome of section 3 and 4
5. Involved border agencies' privacy/legal representatives review completed PIA
6. Subject to feedback, PIA is signed by each border agency approver and privacy/legal reviewer
7. Activity may commence subject to actions or conditions identified in PIA

Section instructions, a glossary at [Appendix 2](#), and explanatory notes at [Appendix 3](#), provide more detail on completing the PIA template. Tables are colour-coded (as above) to indicate who should complete them.

# JOINT BORDER ANALYTICS

## Joint-Agency Privacy Impact Assessment

### 1. Governance and contact information

**What's this for?** This section records which border agencies initiated the analytics activity, the roles of any border agencies involved in the activity, and the contact details for key staff involved. Note, JBAC will always be involved as the analytics service provider.

**Who should complete this?** JBAC will complete this section on behalf of the involved border agencies.

<b>Date PIA commenced</b>	7 July 2020				
<b>JBAC contact person for this activity</b>	§ 9(2)(g)(ii) OIA				
<b>Border agencies involved in this activity</b>	<b>NZCS (non-JBAC)</b>	<b>MPI</b>	<b>MBIE</b>	<b>DIA</b>	<b>DOC</b>
	<input checked="" type="checkbox"/> Lead Agency <input checked="" type="checkbox"/> Data Provider <input checked="" type="checkbox"/> Data Recipient/User	<input type="checkbox"/> Lead Agency <input type="checkbox"/> Data Provider <input type="checkbox"/> Data Recipient/User	<input type="checkbox"/> Lead Agency <input checked="" type="checkbox"/> Data Provider <input checked="" type="checkbox"/> Data Recipient/User	<input type="checkbox"/> Lead Agency <input type="checkbox"/> Data Provider <input type="checkbox"/> Data Recipient/User	<input type="checkbox"/> Lead Agency <input type="checkbox"/> Data Provider <input type="checkbox"/> Data Recipient/User
<b>Activity contact person for each agency</b>	Name: § 9(2)(g) Email: TBC	Name: Email:	Name: § 9(2)(g)(ii) Email: TBC	Name: Email:	Name: Email:
<b>Privacy/legal representative for each agency</b>	Name: § 9(2)(g)(ii) Email: TBC	Name: Email:	Name: § 9(2)(g)(ii) Email: TBC	Name: Email:	Name: Email:

# JOINT BORDER ANALYTICS

## 2. Overview of the activity

**What's this for?** This section explains the analytics activity, for the purpose of assisting the involved border agencies to make data sharing and/or output dissemination assessments.

**Who should complete this?** JBAC will complete this section on behalf of the involved border agencies.

<p><b>1. What is the name of this activity?</b></p>	<p>Shore Parties</p>
<p><b>2. Briefly describe the activity, including the problem/s it is seeking to address</b></p>	<p>'Shore parties' is a coverall reference to persons entering New Zealand for the purpose of facilitating the import and domestic movement of illicit goods, primarily drugs and tobacco. Large imports of illicit drugs have recently been increasing in frequency, and are predominantly linked to trans-national crime syndicates. These syndicates – comprising various shore parties – have evolved into sophisticated groups that utilise advanced modus operandi to exploit the border.</p> <p>The Shore Parties activity aims to better identify existing or potential shore parties, using datasets from NZCS and MBIE. The high-level objectives of the Shore Parties activity are to:</p> <ul style="list-style-type: none"> <li>• provide insights into the risk posed by transnational organised crime groups via shore parties;</li> <li>• inform and improve targeting efforts;</li> <li>• enable more effective use of resource as passenger and goods movements increase; and</li> <li>• enable more effective identification of risk.</li> </ul> <p>s 6(c) OIA</p>

# JOINT BORDER ANALYTICS

	s 6(c) OIA			
<b>3. How does this activity support each Data Recipient/User's lawful purposes and deliver public benefit? [2]</b>	NZCS	Will support NZCS' border enforcement activities, under the Customs and Excise Act, by informing and improving risk targeting efforts, better identifying risk, and enabling more effective use of enforcement resources.		
	MBIE	Will support MBIE's border and on-shore enforcement activities, under the Immigration Act, by informing and improving risk targeting efforts, better identifying risk, and enabling more effective use of enforcement resources.		
<b>4. What datasets are required for this activity? See <a href="#">Appendix 1</a> for more detail</b>	<b>Dataset</b>	<b>Data Provider</b>	<b>Time period</b>	<b>Relevance to activity</b>
	s 6(c) OIA			

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

# JOINT BORDER ANALYTICS

				s 6(c) OIA
5. Where will the analytics dataset be stored and processed? <a href="#">[3]</a>	s 6(c) OIA			
6. How long will the analytics dataset be retained?				
7. What are the <u>intended</u> outputs of this activity?	<input checked="" type="checkbox"/> Analytics models and forecasts (non-identifiable)		<input checked="" type="checkbox"/> Identifiable intelligence outputs <i>If this has been selected, section 4 must be completed</i>	
8. Briefly describe the outputs	s 6(c) OIA			
9. Relevant attached documents				

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

# JOINT BORDER ANALYTICS

## 3. Data sharing assessment

**What's this for?** This section assesses the lawfulness of data sharing required to build the analytics dataset for the activity. Each activity will require the collection and disclosure of personal information by two or more border agencies, and usually all involved agencies will use the analytics dataset for the activity. Where appropriate, explain your answers in the right-hand column.

**Who should complete this?** Each Data Provider and Data Recipient/User identified at section 1 must complete this assessment for each dataset being shared to ensure that they are satisfied they have a lawful basis to share personal information for this activity. Where an activity requires the collection of a third party or publicly available dataset, no Data Provider assessment will be required but each Data Recipient/User must complete a Data Recipient/User assessment for that dataset. An activity may only proceed where all Data Providers and Data Recipients are satisfied that the data sharing is lawful and necessary.

### A. Dataset: Customs datasets

<b>Data Provider</b>	NZCS		
<b>Dataset</b>	s 6(c) OIA		
<b>1. Are you satisfied that you have a lawful basis to disclose this dataset to the Data Recipients? IPP 11 [4]</b>	<input checked="" type="checkbox"/> Principle 11(e)(i) – maintenance of the law [6]	These datasets will be used to develop analytics models and identifiable outputs for the purposes of assisting NZCS and MBIE with their law enforcement activities, including the detection, investigation and prosecution of offences under the Customs and Excise Act and Immigration Act.	Proceed
<b>2. Are you satisfied that the personal information in this dataset – including data fields or time periods – is reasonably necessary for this activity? IPP 1 [8]</b>	<input checked="" type="checkbox"/> Yes, the dataset is necessary	JBAC has established during the data exploration phase that each data field in each dataset is necessary for the purposes of developing the analytics models and identifiable outputs.	Proceed
<b>3. Are there any statutory restrictions on the use or retention of some or all of the information in the dataset?</b>	<input checked="" type="checkbox"/> Yes	s 6(c) OIA	Action required

# JOINT BORDER ANALYTICS

		s 6(c) OIA	
4. Have reasonable steps been taken to ensure the dataset is accurate and up-to-date before it is disclosed? IPP 8	<input checked="" type="checkbox"/> Yes, reasonable steps have been taken		Proceed
5. Privacy/Legal team comments			
6. Can the disclosure of this dataset proceed?	<input checked="" type="checkbox"/> Yes, but:	<input checked="" type="checkbox"/> We need to address statutory restrictions	

Data Recipient/User	NZCS		
Dataset	s 6(c) OIA		
1. Are you satisfied that you have a lawful basis to collect this dataset from the Data Provider? IPP 2 [4]	<input checked="" type="checkbox"/> It's our dataset, we're not collecting it	N/A	Proceed
2. Are you satisfied that the personal information in this dataset – including data fields or time periods – is reasonably necessary for this activity? IPP 1 [8]	<input checked="" type="checkbox"/> Yes, the dataset is necessary	JBAC has established during the data exploration phase that each data field in each dataset is necessary for the purposes of developing the analytics models and identifiable outputs.	Proceed
3. Could the people this data relates to view this collection as unfair or unreasonably intrusive? IPP 4 [12]	<input checked="" type="checkbox"/> It's our dataset, we're not collecting it	N/A	Proceed
4. Are you satisfied that you have a lawful basis to use this dataset for the	<input checked="" type="checkbox"/> Our enabling legislation	As we already hold these datasets, we are satisfied that using them for the purposes of developing analytics models and identifiable outputs as data	Proceed

# JOINT BORDER ANALYTICS

purpose of this analytics activity? IPP 10 [4]		as outlined above is aligned with our lawful border purposes under section 301 of the C&E Act. This s 6(c) OIA [REDACTED]	
	<input checked="" type="checkbox"/> Principle 10(c)(i) – maintenance of the law [14]	In addition, we are satisfied that the use of these datasets is permitted by the maintenance of the law exception to IPP 10, for the reasons outlined above.	Proceed
5. Privacy/Legal team comments			
6. Can the collection and use of this dataset proceed?	<input checked="" type="checkbox"/> Yes - Approved by: Name		

Data Recipient/User	MBIE		
Dataset	s 6(c) OIA [REDACTED]		
1. Are you satisfied that you have a lawful basis to collect this dataset from the Data Provider? IPP 2 [4]	<input checked="" type="checkbox"/> Principle 2(2)(d)(i) – maintenance of the law [10]	These datasets will be used to develop analytics models and identifiable outputs for the purposes of assisting NZCS and MBIE with their law enforcement activities, including the detection, investigation and prosecution of offences under the Customs and Excise Act and Immigration Act.	Proceed
2. Are you satisfied that the personal information in this dataset – including data fields or time periods – is reasonably necessary for this activity? IPP 1 [8]	<input checked="" type="checkbox"/> Yes, the dataset is necessary	JBAC has established during the data exploration phase that each data field in each dataset is necessary for the purposes of developing the analytics models and identifiable outputs.	Proceed



# JOINT BORDER ANALYTICS

3. Could the people this data relates to view this collection as unfair or unreasonably intrusive? IPP 4 [12]	<input checked="" type="checkbox"/> No	We are satisfied that the collection of these datasets is proportional, particularly in view of the process already applied to explore and refine the data.	Proceed
4. Are you satisfied that you have a lawful basis to use this dataset for the purpose of this analytics activity? IPP 10 [4]	<input checked="" type="checkbox"/> Principle 10(c)(i) – maintenance of the law [14]	We are satisfied that the use of these datasets is permitted by the maintenance of the law exception to IPP 10, for the reasons outlined above.	Proceed
	<input checked="" type="checkbox"/> Other	Note, section 33 of the Immigration Act permits us to use classified information to make decisions under the Act (including in relation to visas) if it relates to matters of security or criminal conduct. However, if this activity ultimately results in the development of classified identifiable outputs, we must ensure that our use of these outputs complies with sections 34-40 of the Immigration Act.	Proceed
5. Privacy/Legal team comments			
6. Can the collection and use of this dataset proceed?	<input checked="" type="checkbox"/> Yes - Approved by: Name		

## B. Dataset: INZ datasets

Data Provider	MBIE		
Dataset	s 6(c) OIA		
1. Are you satisfied that you have a lawful basis to disclose this dataset to the Data Recipients? IPP 11 [4]	<input checked="" type="checkbox"/> Principle 11(e)(i) – maintenance of the law [6]	This dataset will be used to develop analytics models and identifiable outputs for the purposes of assisting NZCS and MBIE with their law enforcement activities, including the detection,	Proceed

# JOINT BORDER ANALYTICS

		investigation and prosecution of offences under the Customs and Excise Act and Immigration Act.	
<b>2. Are you satisfied that the personal information in this dataset – including data fields or time periods – is reasonably necessary for this activity?</b> IPP 1 [8]	<input checked="" type="checkbox"/> Yes, the dataset is necessary	JBAC has established during the data exploration phase that each data field s 6(c) OIA [REDACTED] in this dataset is necessary for the purposes of developing the analytics models and identifiable outputs.	Proceed
<b>3. Are there any statutory restrictions on the use or retention of some or all of the information in the dataset?</b>	<input checked="" type="checkbox"/> No	N/A	Proceed
<b>4. Have reasonable steps been taken to ensure the dataset is accurate and up-to-date before it is disclosed?</b> IPP 8	<input checked="" type="checkbox"/> Yes, reasonable steps have been taken	In view of the fact that the dataset will be refreshed on a regular basis to ensure it is up to date, and will be subject to a cleansing and matching process, we are satisfied that no further steps are required before sharing it.	Proceed
<b>5. Privacy/Legal team comments</b>			
<b>6. Can the disclosure of this dataset proceed?</b>	<input checked="" type="checkbox"/> Yes - Approved by: Name		

<b>Data Recipient/User</b>	MBIE		
<b>Dataset</b>	s 6(c) OIA [REDACTED]		
<b>1. Are you satisfied that you have a lawful basis to collect this dataset from the Data Provider?</b> IPP 2 [4]	<input checked="" type="checkbox"/> It's our dataset, we're not collecting it	N/A	Proceed
<b>2. Are you satisfied that the personal information in this dataset – including data fields or time periods – is</b>	<input checked="" type="checkbox"/> Yes, the dataset is necessary	JBAC has established during the data exploration phase that each data field s 6(c) OIA [REDACTED] in	Proceed

# JOINT BORDER ANALYTICS

reasonably necessary for this activity? IPP 1 [8]		this dataset is necessary for the purposes of developing the analytics models and identifiable outputs.	
3. Could the people this data relates to view this collection as unfair or unreasonably intrusive? IPP 4 [12]	<input checked="" type="checkbox"/> It's our dataset, we're not collecting it	N/A	Proceed
4. Are you satisfied that you have a lawful basis to use this dataset for the purpose of this analytics activity? IPP 10 [4]	<input checked="" type="checkbox"/> Principle 10(c)(i) – maintenance of the law [14]	We are satisfied that the use of this dataset is permitted by the maintenance of the law exception to IPP 10, for the reasons outlined above.	Proceed
	<input checked="" type="checkbox"/> Other	We are also satisfied that, as this is MBIE data, our use of the dataset for the purposes of generating analytical outputs that should assist with our law enforcement activities aligns with the purposes for which we collected this data.	Proceed
5. Privacy/Legal team comments			
6. Can the collection and use of this dataset proceed?	<input checked="" type="checkbox"/> Yes - Approved by: Name		

Data Recipient/User	NZCS		
Dataset	s 6(c) OIA		
1. Are you satisfied that you have a lawful basis to collect this dataset from the Data Provider? IPP 2 [4]	<input checked="" type="checkbox"/> Principle 2(2)(d)(i) – maintenance of the law [10]	This dataset will be used to develop analytics models and identifiable outputs for the purposes of assisting NZCS and MBIE with their law enforcement activities, including the detection, investigation and prosecution of offences under the Customs and Excise Act and Immigration Act.	Proceed

# JOINT BORDER ANALYTICS

<p>2. Are you satisfied that the personal information in this dataset – including data fields or time periods – is reasonably necessary for this activity? IPP 1 [8]</p>	<input checked="" type="checkbox"/> Yes, the dataset is necessary	<p>JBAC has established during the data exploration phase that each data field s 6(c) OIA [REDACTED] in this dataset is necessary for the purposes of developing the analytics models and identifiable outputs.</p>	<p>Proceed</p>
<p>3. Could the people this data relates to view this collection as unfair or unreasonably intrusive? IPP 4 [12]</p>	<input checked="" type="checkbox"/> No		<p>Proceed</p>
<p>4. Are you satisfied that you have a lawful basis to use this dataset for the purpose of this analytics activity? IPP 10 [4]</p>	<input checked="" type="checkbox"/> Our enabling legislation	<p>Section 301(2) of the C&amp;E Act permits NZCS to use any information provided to it for a lawful purpose related to its legislative functions functions (section 301(1)(a)(ii) of the C&amp;E Act) for any lawful purpose related to its legislative functions. This would include using this data to develop analytic models and identifiable outputs that will support our lawful border purposes.</p>	<p>Proceed</p>
	<input checked="" type="checkbox"/> Principle 10(c)(i) – maintenance of the law [14]	<p>In addition, we are satisfied that the use of this dataset is permitted by the maintenance of the law exception to IPP 10, for the reasons outlined above.</p>	<p>Proceed</p>
<p>5. Privacy/Legal team comments</p>			
<p>6. Can the collection and use of this dataset proceed?</p>	<input checked="" type="checkbox"/> Yes - Approved by: Name		

## C. Dataset: Companies Office datasets

<p>Data Provider</p>	<p>MBIE</p>
<p>Dataset</p>	<p>s 6(c) OIA [REDACTED]</p>

# JOINT BORDER ANALYTICS

<p>1. Are you satisfied that you have a lawful basis to disclose this dataset to the Data Recipients? IPP 11 [4]</p>	<input checked="" type="checkbox"/> Principle 11(e)(i) – maintenance of the law [6]	<p>These datasets will be used to develop analytics models and identifiable outputs for the purposes of assisting NZCS and MBIE with their law enforcement activities, including the detection, investigation and prosecution of offences under the Customs and Excise Act and Immigration Act.</p>	<p>Proceed</p>
<p>2. Are you satisfied that the personal information in this dataset – including data fields or time periods – is reasonably necessary for this activity? IPP 1 [8]</p>	<input checked="" type="checkbox"/> Yes, the dataset is necessary	<p>JBAC has established during the data exploration phase that each data field in each dataset is necessary for the purposes of developing the analytics models and identifiable outputs.</p>	<p>Proceed</p>
<p>3. Are there any statutory restrictions on the use or retention of some or all of the information in the dataset?</p>	<input checked="" type="checkbox"/> Yes	<p>s 6(c) OIA</p>	<p>Action required</p>
<p>4. Have reasonable steps been taken to ensure the dataset is accurate and up-to-date before it is disclosed? IPP 8</p>	<input checked="" type="checkbox"/> Yes, reasonable steps have been taken		<p>Proceed</p>
<p>5. Privacy/Legal team comments</p>			
<p>6. Can the disclosure of this dataset proceed?</p>	<input checked="" type="checkbox"/> Yes, but:	<input checked="" type="checkbox"/> We need to address statutory restrictions	

# JOINT BORDER ANALYTICS

Data Recipient/User	MBIE		
Dataset	s 6(c) OIA		
1. Are you satisfied that you have a lawful basis to collect this dataset from the Data Provider? IPP 2 [4]	<input checked="" type="checkbox"/> Principle 2(2)(d)(i) – maintenance of the law [10]	s 6(c) OIA  We are satisfied that the collection of these datasets is permitted by the maintenance of the law exception to IPP 2, for the reasons outlined above.	Proceed
2. Are you satisfied that the personal information in this dataset – including data fields or time periods – is reasonably necessary for this activity? IPP 1 [8]	<input checked="" type="checkbox"/> Yes, the dataset is necessary	JBAC has established during the data exploration phase that each data field in each dataset is necessary for the purposes of developing the analytics models and identifiable outputs.	Proceed
3. Could the people this data relates to view this collection as unfair or unreasonably intrusive? IPP 4 [12]	<input checked="" type="checkbox"/> No		Proceed
4. Are you satisfied that you have a lawful basis to use this dataset for the purpose of this analytics activity? IPP 10 [4]	<input checked="" type="checkbox"/> Principle 10(c)(i) – maintenance of the law [14]	We are satisfied that the use of these datasets is permitted by the maintenance of the law exception to IPP 10, for the reasons outlined above.	Proceed
5. Privacy/Legal team comments			
6. Can the collection and use of this dataset proceed?	<input checked="" type="checkbox"/> Yes - Approved by: Name		

Data Recipient/User	NZCS
---------------------	------

# JOINT BORDER ANALYTICS

Dataset	s 6(c) OIA		
<b>1. Are you satisfied that you have a lawful basis to collect this dataset from the Data Provider?</b> IPP 2 [4]	<input checked="" type="checkbox"/> Principle 2(2)(d)(i) – maintenance of the law [10]	These datasets will be used to develop analytics models and identifiable outputs for the purposes of assisting NZCS and MBIE with their law enforcement activities, including the detection, investigation and prosecution of offences under the Customs and Excise Act and Immigration Act.	Proceed
<b>2. Are you satisfied that the personal information in this dataset – including data fields or time periods – is reasonably necessary for this activity?</b> IPP 1 [8]	<input checked="" type="checkbox"/> Yes, the dataset is necessary	JBAC has established during the data exploration phase that each data field in each dataset is necessary for the purposes of developing the analytics models and identifiable outputs.	Proceed
<b>3. Could the people this data relates to view this collection as unfair or unreasonably intrusive?</b> IPP 4 [12]	<input checked="" type="checkbox"/> No		Proceed
<b>4. Are you satisfied that you have a lawful basis to use this dataset for the purpose of this analytics activity?</b> IPP 10 [4]	<input checked="" type="checkbox"/> Our enabling legislation	Section 301(2) of the C&E Act permits NZCS to use any information provided to it for a lawful purpose related to its legislative functions (section 301(1)(a)(ii) of the C&E Act) for any lawful purpose related to its legislative functions. This would include using this data to develop analytic models and identifiable outputs that will support our lawful border purposes.	Proceed
	<input checked="" type="checkbox"/> Principle 10(c)(i) – maintenance of the law [14]	In addition, we are satisfied that the use of these datasets is permitted by the maintenance of the law exception to IPP 10, for the reasons outlined above.	Proceed
<b>5. Privacy/Legal team comments</b>			

# JOINT BORDER ANALYTICS

<b>6. Can the collection and use of this dataset proceed?</b>	<input checked="" type="checkbox"/> Yes - Approved by: Name
---------------------------------------------------------------	-------------------------------------------------------------

## 4. Output dissemination assessment

**What's this for?** This section must be completed where an activity will product **identifiable intelligence** outputs, whether these were planned at the outset or have been identified during an activity. This section assesses the lawfulness, fairness, proportionality and necessity of identifiable outputs.

**Who should complete this?** JBAC will complete the overview of the outputs, as the analytics SME. **Each involved border agency that will receive the identifiable intelligence outputs** must complete this assessment for each output being shared to ensure that they are satisfied they have a lawful basis to use it. JBA may only share identifiable intelligence outputs where all involved agencies are satisfied that the output is lawful, fair, proportionate and necessary.

### A. Output: Shore Parties identifiable intelligence output

<b>1. Briefly describe the output</b>	JBAC will use the final refined datasets assessed above, and the analytics model developed with them, to create identifiable lists of people or entities that are possible shore parties. <span style="background-color: black; color: white;">§ 6(c) OIA</span>
<b>2. What personal information will the output include?</b>	<span style="background-color: black; color: white;">[REDACTED]</span>



# JOINT BORDER ANALYTICS

	<p>s 6(c) OIA</p>				
<p><b>3. Which involved agencies will receive the output?</b></p>	<input checked="" type="checkbox"/> NZCS	<input type="checkbox"/> MPI	<input checked="" type="checkbox"/> MBIE	<input type="checkbox"/> DIA	<input type="checkbox"/> DOC
<p><b>4. What security classifications or handling caveats will be applied to this output? [16]</b></p>	<p>The identifiable outputs will be security classified as IN CONFIDENCE.          Handling caveats will be attached to the identifiable outputs that state:</p> <ul style="list-style-type: none"> <li>- Outputs may only be used for the purposes of the receiving agency's statutory law enforcement activities</li> <li>- Outputs must be assessed and validated before use, and intelligence officers must not make enforcement decisions based solely on these outputs</li> <li>- Outputs must not be disclosed further without the authorisation of a recipient agency Intelligence Manager</li> </ul>				
<p><b>5. What steps has JBAC taken to ensure the data used to generate the output is accurate and up-to-date? [17]</b></p>	<p>s 6(c) OIA</p>				
<p><b>6. Briefly describe the algorithm used to generate the output, including the determinative data fields [18]</b></p>	<p>s 6(c) OIA</p>				

# JOINT BORDER ANALYTICS

	s 6(c) OIA
<b>7. What steps have been taken to ensure the datasets are free from unwanted bias? <a href="#">[19]</a></b>	
<b>8. What steps have been taken to ensure the analytics or outputs are not unlawfully discriminatory? <a href="#">[20]</a></b>	

# JOINT BORDER ANALYTICS

	s 6(c) OIA
--	------------

Output recipient	NZCS		
1. Are you satisfied that you have a lawful basis to use the personal information contained in this output? IPP 10 [4]	<input checked="" type="checkbox"/> Our enabling legislation	Section 301(2) of the C&E Act permits NZCS to use any information provided to it for a lawful purpose related to its legislative functions (section 301(1)(a)(ii) of the C&E Act) for any lawful purpose related to its legislative functions. This would include using these identifiable outputs to inform our law enforcement activities at the border.	Proceed
	<input checked="" type="checkbox"/> Principle 10(c)(i) – maintenance of the law [14]	In addition, we are satisfied that the use of these identifiable outputs is permitted by the maintenance of the law exception to IPP 10, for the reasons outlined above.	Proceed
2. Are you satisfied that the output is relevant to your lawful purposes? [21]	<input checked="" type="checkbox"/> Yes, it is relevant	This identifiable output will directly identify possible shore parties, which will inform our border enforcement activities and targeting efforts. This output is highly relevant to our lawful purposes.	Proceed
3. Are you satisfied that this output is proportionate to the problem it is intended to address? [22]	<input checked="" type="checkbox"/> Yes, it is proportional	This output is intended to assist NZCS to better detect and prevent the importing of illicit drugs and tobacco by shore parties. These are serious crimes that have a significant impact on our communities. In view of the seriousness of these crimes and the harm they cause, this output is proportionate.	Proceed

# JOINT BORDER ANALYTICS

<p>4. Are you satisfied that sufficient steps are in place to protect against unwanted bias or unlawful discrimination? <a href="#">[19]</a> <a href="#">[20]</a></p>	<input checked="" type="checkbox"/> Yes, we are satisfied	<p>In our view the datasets themselves would appear to contain no biases, as they are entire factual records of NZCS and MBIE interactions with the entities and individuals. The datasets have not been selected or refined based on existing biases.</p> <p>The risk factors or predictors are broad and it is clear that individuals will not be identified as shore parties (and therefore potentially subjected to adverse action) solely on the basis of a prohibited ground.</p>	<p>Proceed</p>
<p>5. Are you satisfied that the outputs will be appropriately classified or caveated?</p>	<input checked="" type="checkbox"/> No, we are not satisfied	<p>Appropriate security classifications need to be assigned to the identifiable outputs. We think this should be set at RESTRICTED.</p>	<p><b>Action required</b></p>
<p>6. Do you have processes in place to ensure that this output is validated before being relied upon to take adverse actions?</p>	<input checked="" type="checkbox"/> Yes, we do	<p>TBC</p>	<p>Proceed</p>
<p>7. Do you have processes in place to ensure that individuals can challenge any adverse actions taken on the basis of this output?</p>	<input checked="" type="checkbox"/> Yes, we do	<p>TBC</p>	<p>Proceed</p>
<p>8. Privacy/Legal team comments</p>			
<p>9. Can the output proceed as intended?</p>	<input checked="" type="checkbox"/> <b>Yes, but:</b> <input checked="" type="checkbox"/> The output needs to be correctly classified or caveated		
<p><b>Output recipient</b></p>			
<p>MBIE</p>			
<p>1. Are you satisfied that you have a lawful basis to use the personal information contained in this output? <i>IPP 10</i> <a href="#">[4]</a></p>	<input checked="" type="checkbox"/> No, we do not think there is a lawful basis	<p>We are not satisfied that the identifiable output is sufficiently relevant to our law enforcement activities to warrant the release of identifiable</p>	<p><b>Action required</b></p>

# JOINT BORDER ANALYTICS

		information generated by this analytics activity to MBIE.	
2. Are you satisfied that the output is relevant to your lawful purposes? <a href="#">[21]</a>	<input checked="" type="checkbox"/> No, it is not relevant	As above	Action required
8. Privacy/Legal team comments			
9. Can the output proceed as intended?	<input checked="" type="checkbox"/> No, because:	<input checked="" type="checkbox"/> We have no lawful basis to use <input checked="" type="checkbox"/> The output is not relevant to our lawful purposes	

## 5. Privacy risks, mitigations and actions

*This section captures any risks generated by the outcomes of sections 3 and 4. JBA or the border agencies can also add more risks and mitigations here. Some risks that cannot be mitigated will require an action (such as removing a Data Recipient where no lawful basis can be established to include them) and others will require mitigations (such as refining data requirements, establishing data destruction rules or data refresh processes).*

**What's this for?**

**Who should complete this?** JBAC will complete this section on behalf of the border agencies but **border agencies** may also add content as required.

Risk	Mitigation/Action	Responsible	Date complete
R3 <input checked="" type="checkbox"/> There are statutory restrictions that must be met	s 6(c) OIA	JBAC	
R3 <input checked="" type="checkbox"/> There are statutory restrictions that must be met		JBAC	

# JOINT BORDER ANALYTICS

R8 <input checked="" type="checkbox"/> A Data Recipient/User has no lawful basis to use an identifiable intelligence output	MBIE is not satisfied that the identifiable output is relevant to its law enforcement purposes. The identifiable output must not be shared with MBIE.	JBAC	
R9 <input checked="" type="checkbox"/> An identifiable intelligence output is not relevant to one of the Data Recipients/Users	MBIE is not satisfied that the identifiable output is relevant to its law enforcement purposes. The identifiable output must not be shared with MBIE.	JBAC	
R14 <input checked="" type="checkbox"/> An identifiable intelligence output has not been correctly classified or caveated	The identifiable output needs to be appropriately classified. It is recommended, in the circumstances, that it be classified as RESTRICTED. Add a handling caveat that stipulates the identifiable output should not be shared with MBIE	JBAC	

## 6. Activity Sign off

**What's this for?**

*This section captures border agency approval for the activity and also records that this PIA has been reviewed by the border agency's Privacy Officer or team. An activity cannot proceed until this section has been completed in full by all involved border agencies.*

**Who should complete this?**

*For activities that will not result in identifiable intelligence outputs, border agency approval must be **manager level or above**. For activities that will result in identifiable intelligence outputs, border agency approval must be **Chief Executive level or above**.*

Border agency	NZCS		
Activity approved by		Privacy review by	
Name:	Name:		
Position:	Position:		
Date:	Date:		

Border agency	MBIE		
---------------	------	--	--

# JOINT BORDER ANALYTICS

Activity approved by	Privacy review by
Name: Position: Date:	Name: Position: Date:

JBAC
PIA reviewed by
s 9(2)(g)(ii) OIA Date:

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

# JOINT BORDER ANALYTICS

## Appendix 1: Data fields

**What's this for?**

*This section identifies the data fields contained in each dataset that has been identified as necessary for the activity. This will assist the border agencies to assess the lawfulness of the data sharing required to enable the activity.*

**Who should complete this?**

*JBAC will complete this section on behalf of the involved border agencies.*


Dataset	Data source	Time period	Description	Relevance to activity
s 6(c) OIA				

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982



# JOINT BORDER ANALYTICS

s 6(c) OIA



RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

# JOINT BORDER ANALYTICS

## Appendix 2: Glossary

This	Means
<b>Activity</b>	an agreed and authorised (by the involved border agencies) use of data analytics to produce a set of outputs that may include analytics models, forecasts or identifiable intelligence outputs.
<b>Adverse action</b>	any action that may adversely affect the rights, benefits, privileges, obligations, or interests of any specific individual; including any decision: <ol style="list-style-type: none"> <li>i. to make an assessment of the amount of any tax, levy, or other charge, or of any contribution, that is payable by any individual, or to alter any such assessment:</li> <li>ii. to investigate the possible commission of an offence:</li> <li>iii. to make a deportation order in relation to the individual, to serve the individual with a deportation liability notice, or to deport the individual from New Zealand.</li> </ol>
<b>Analytics forecasts</b>	forecasts designed to look forward at possible future patterns of border risk using historical information. These products contain no personal information.
<b>Analytics models</b>	models that identify a <u>class</u> of goods, craft and/or people who present an increased or decreased risk at the border. The output of analytics models offers a score based on weighted predictors. These products contain no personal information but may be used by border agencies to create personal information (as a result of running the model).
<b>Border agency</b>	DIA, DOC, MBIE, MPI or NZCS.
<b>CRISP-DM</b>	Cross Industry Standard Process for Data Science (CRISP-DM). CRISP-DM is an open standard process model that describes common approaches used by data mining experts. It has six stages – business understanding, data understanding, data preparation, modelling, evaluation, and deployment.
<b>Data analytics</b>	the discovery, interpretation, and communication of meaningful patterns in data.
<b>Data exploration</b>	the comparison of datasets and data fields through the use of analytical techniques, methods and modelling, in order to better understand the relationship between datasets or data fields for the purposes of generating analytics outputs.
<b>Data Provider</b>	the border agency which has been requested to disclose a dataset to other border agencies for the purpose of a joint-agency analytics activity.
<b>Data Recipient/User</b>	the border agency which will collect and use a dataset or identifiable output as part of a joint-agency analytics activity.

# JOINT BORDER ANALYTICS

<b>Data refinement</b>	the possible result of the data exploration process, where datasets or data fields found not to be relevant to desired outputs are purged from the analytics dataset.
<b>Data sharing</b>	the disclosure of personal information by one border agency to one or more other border agencies and the collection of personal information by one border agency from one or more other border agencies.
<b>Dataset</b>	a distinct category of data held by an involved border agency, by a third-party agency or that is publicly available. Each dataset will include data fields that may relate to identifiable individuals.
<b>DIA</b>	Department of Internal Affairs.
<b>DOC</b>	Department of Conservation.
<b>Enabling legislation</b>	the legislation which sets out a border agency's statutory functions and powers and includes the Customs and Excise Act 2018, Biosecurity Act 1993 and Immigration Act 2009.
<b>Identifiable intelligence outputs</b>	the result of an analytical process which produces identifiable information. The output may identify previously unknown relationships or indicate a known or unknown level of risk for an individual.
<b>JBAC</b>	Joint Border Analytics Centre; MPI, NZCS and MBIE/Immigration analytics experts delivering technical solutions and insights at the request of border agencies. The team is operationally focused.
<b>Lead Agency</b>	the border agency that has initiated the activity, will provide the platform within which the activity will be completed, and must be a Data Recipient/User for the activity.
<b>Personal information</b>	any information about an identifiable individual (natural person), including but not limited to personal identifiers (like name and address) and any information linked to personal identifiers (like events or entities). By combining datasets and linking fields with certain individuals (for example using the IR Number or name and address), analytics activities may create new personal information about identifiable individuals.
<b>MBIE</b>	Ministry of Business, Innovation and Employment, which includes Immigration New Zealand.
<b>MPI</b>	Ministry for Primary Industries.
<b>MOU</b>	the Joint Border Analytics Memorandum of Understanding, signed by all involved border agencies and the JBAC Team.
<b>NZCS</b>	New Zealand Customs Service.
<b>Unlawful discrimination</b>	discrimination based on any grounds prohibited by the Human Rights Act 1993, including sex, marital status, religious belief, colour, race, ethnic origin, disability, age, political opinion, and sexual orientation.

# JOINT BORDER ANALYTICS

## Appendix 3: Explanatory Notes

[1] In the absence of specific legislation that permits border agencies to collect or disclose personal information, the Privacy Act and IPPs apply. The IPPs are a flexible set of principles intended to ensure that agencies can achieve their goals in a privacy protective way. In summary, they require an agency to:

1. **Scope** – Collect only the personal information it needs for a lawful purpose connected with its functions.
2. **Source** – Collect personal information directly from the person concerned, unless an exception applies.
3. **Notice** – Tell people certain things when collecting personal information directly from them.
4. **Manner** – Collect personal information in ways that are lawful and, in the circumstances, fair and not unreasonably intrusive.
5. **Security** – Take reasonable steps to protect personal information from harm.
6. **Subject access** – Give people access to the personal information it holds about them.
7. **Correction** – Let people correct personal information if it is incorrect.
8. **Accuracy** – Take reasonable steps to ensure personal information is accurate and up-to-date before using it.
9. **Retention** – Retain personal information for no longer than is required.
10. **Use** – Use personal information only for the purposes for which it was collected, unless an exception applies.
11. **Disclosure** – Not disclose personal information, unless an exception applies.
12. **Unique identifiers** – Take care when assigning or using unique identifiers.

Many IPPs – including principles 2 and 10 – contain exceptions that ensure legitimate information processing is possible. Thus, even where a border agency's enabling legislation is silent on the matter of sharing or using personal information for analytics activities, the Privacy Act is likely to permit it, provided that it is necessary and proportional and relates to the involved agencies' lawful functions.

The Privacy Commissioner and Government Chief Data Steward released a set of *principles for the safe and effective use of data and analytics* ('Analytics Principles'), intended to promote transparency and a best-practice approach to the use of data and analytics for supporting operational decision-making.

1. **Deliver clear public benefit** – it's essential government agencies consider, and can demonstrate, positive public benefits from collecting and using public data.
2. **Ensure data is fit for purpose** – using the right data in the right context can substantially improve decision-making and analytical models, and will avoid generating potentially harmful outcomes.
3. **Focus on people** – keep in mind the people behind the data and how to protect them against misuse of information.
4. **Maintain transparency** – transparency is essential for accountability. It supports collaboration, partnership, and shared responsibility.
5. **Understand the limitations** – while data is a powerful tool, all analytical processes have inherent limitations in their ability to predict and describe outcomes.
6. **Retain human oversight** – analytical processes are a tool to inform human decision-making and should never entirely replace human oversight.

[2] It is essential that the involved border agencies consider, and can demonstrate, positive **public benefits** from collecting, analysing and using personal information. A clear link to an involved agency's lawful purposes (as set out in its enabling legislation) is also required to ensure that an activity is legitimate and necessary.

# JOINT BORDER ANALYTICS

- [3] Analytics datasets relating to joint-agency analytics activities will usually be **stored and processed** within the Lead Agency's system, in accordance with the JBA MOU and joint-agency SOPs. Where JBAC proposes to store or process datasets on another platform, this must be stated in the PIA.
- [4] The burden of establishing that an exception applies to permit a disclosure, collection or use of personal information rests with the border agency seeking to rely on it. An involved border agency may seek further clarity from JBAC or the other involved border agencies where this is required in order to establish whether an exception applies.
- [5] Principle 11(h)(ii) permits the disclosure of personal information if the information is to be used for statistical or research purposes and will not be published in an identifiable form. This exception is likely to permit the disclosure of relevant personal information for the purposes of generating analytics models and forecasts, but should not be applied where the involved border agencies intend to generate identifiable intelligence outputs.
- [6] Principle 11(e)(i) permits the disclosure of personal information where this is necessary to avoid prejudice to the maintenance of the law, including the prevention, detection, investigation, and prosecution of offences. This exception is likely to permit the disclosure of relevant personal information for the purposes of generating targeted analytics forecasts (intended to detect or prevent offences) or identifiable intelligence outputs. Note, 'necessity' includes considerations of data minimisation and proportionality.
- [7] Principle 11(f) permits the disclosure of personal information where this is necessary to prevent or lessen a serious threat to public health or safety or the life or health of an individual. This exception may permit the disclosure of relevant personal information for the purposes of generating or disseminating identifiable intelligence outputs to respond to an imminent threat.
- [8] **Data minimisation** is an important element of the privacy framework. Agencies should disclose, collect and use only the minimum amount of personal information necessary to meet their lawful purposes. In the initial stages of an analytics activity, lawful purposes will include exploring and assessing datasets available to establish how useful each will be. Effort should be made initially to ensure that exploration datasets shared are broadly relevant to the activity and, later, to remove any datasets or data fields that are not found to be relevant to the activity.
- [9] Principle 2(2)(g)(ii) permits the collection of personal information if the information is to be used for statistical or research purposes and will not be published in an identifiable form. This exception is likely to permit the collection of relevant personal information for the purposes of generating analytics models and forecasts, but should not be applied where the involved border agencies intend to generate identifiable intelligence outputs.
- [10] Principle 2(2)(d)(i) permits the collection of personal information where this is necessary to avoid prejudice to the maintenance of the law, including the prevention, detection, investigation, and prosecution of offences. This exception is likely to permit the collection of relevant personal information for the purposes of generating targeted analytics forecasts (intended to detect or prevent offences) or identifiable intelligence outputs. Note, 'necessity' includes considerations of data minimisation and proportionality.
- [11] Principle 2 will be amended by the Privacy Bill to include a serious threat exception. Once amended, this exception will permit the collection of personal information where this is necessary to prevent or lessen a serious threat to public health or safety or the life or health of an individual. This exception may permit the collection of relevant personal information for the purposes of generating or disseminating identifiable intelligence outputs to respond to an imminent threat.

# JOINT BORDER ANALYTICS

- [12] Principle 4 requires an agency to collect personal information in a manner that is not unlawful or, in the circumstances, unfair or unreasonably intrusive. This principle incorporates concepts of fairness and proportionality, and will require Data Recipients/Users to consider whether the collection of a dataset for the purposes of a particular analytics activity could be viewed as unfair or intruding into the personal affairs of affected individuals to a greater extent than the ends would justify.
- [13] Principle 10(f)(ii) permits the use of personal information if the information is to be used for statistical or research purposes and will not be published in an identifiable form. This exception is likely to permit the use of relevant personal information for the purposes of generating analytics models and forecasts, but should not be applied where the involved border agencies intend to generate identifiable intelligence outputs.
- [14] Principle 10(c)(i) permits the use of personal information where this is necessary to avoid prejudice to the maintenance of the law, including the prevention, detection, investigation, and prosecution of offences. This exception is likely to permit the use of relevant personal information for the purposes of generating targeted analytics forecasts (intended to detect or prevent offences) or identifiable intelligence outputs.
- [15] Principle 10(d) permits the use of personal information where this is necessary to prevent or lessen a serious threat to public health or safety or the life or health of an individual. This exception may permit the use of relevant personal information for the purposes of generating or disseminating identifiable intelligence outputs to respond to an imminent threat.
- [16] **Handling caveats** are an effective way to manage the use or disclosure of identifiable outputs, particularly where these outputs may be sensitive. Handling caveats might include a requirement that the output is used only for intelligence purposes, that the output is retained only for a set period of time, or that the output recipient must obtain JBAC approval before sharing the output further.
- [17] **Accuracy steps** might include regularly refreshing the datasets used for generating the outputs, and ensuring that information is correctly matched (for example where an identifiable individual is matched with a non-compliant entity or event).
- [18] **Algorithmic transparency** is an important element of fairness and due process. JBAC must be able to explain to involved border agencies how an algorithm has identified a particular individual as high risk. This will assist the border agency to assess the lawfulness and proportionality of the analytics activity and to provide affected individuals with a meaningful process for challenging decisions made as a result of analytics.
- [19] JBAC should assist border agencies to ensure that **unwanted biases** are removed from datasets before they are analysed, recognising that some lawful bias may be legitimate in certain circumstances, to ensure that an activity is properly targeting known risk groups or attributes.
- [20] Border agency law enforcement activities are subject to section 19 of the Bill of Rights Act, which provides the right to be free from discrimination based on a prohibited ground (**unlawful discrimination** is defined in the glossary). While some prohibited grounds – such as age, political opinion or ethnic origin – may in certain cases be relevant to risk, analytics should not be designed to profile risk solely on the basis of a prohibited ground.
- [21] Each Data Recipient/User must ensure that it only receives identifiable intelligence outputs that are **relevant** to its lawful purposes. For example, an intelligence product that indicates identified individuals who pose a risk of a specific Customs and Excise Act offence may not be of any relevance to Immigration Intelligence Officers looking to prevent specific Immigration Act offences.

# JOINT BORDER ANALYTICS

[22] As stated at note [12] above, involved border agencies must ensure that the intrusiveness of the data analytics and intelligence outputs is warranted, and **proportionate** to the problem the activity is seeking to address. This could be assessed by reference to the severity of the border risk or level of offending being targeted by the activity.

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1082