JOINT BORDER ANALYTICS

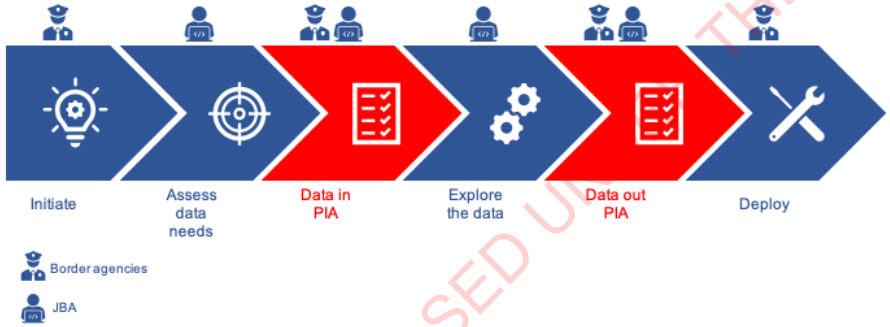
Single Agency Privacy Impact Assessment Template – DATA OUT module

This module is for any new single agency analytics activity, conducted by the Joint Border Analytics Centre (JBAC) on behalf of a border agency, that will produce identifiable intelligence outputs. The module assists the requesting border agency to assess the lawfulness, necessity and relevance of any identifiable intelligence outputs produced as a result of the activity. [1]

The objective of the JBAC PIA process and modules is to **enable single 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

Single agency analytics activities must be initiated by a border agency (the Requesting Agency). The Requesting Agency is responsible for assessing privacy or other risks raised by an activity and approving the activity. The Requesting 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 analytics activities or outputs.



What the PIA covers

This is a DATA OUT PIA module. A new module must be completed for each identifiable intelligence output that may be produced by JBAC on behalf of the Requesting Agency.

The process in brief

1. Requesting Agency initiates analytics activity with JBAC
2. JBAC completes sections 1 and 2 (in consultation with the Requesting Agency)
3. Requesting Agency completes section 3 (in consultation with JBAC)
4. JBAC completes section 4 to reflect outcome of section 3
5. Requesting Agency's privacy/legal representatives review completed PIA and add feedback
6. Subject to feedback, PIA is signed by Requesting Agency and privacy/legal reviewer
7. Activity may commence subject to actions or conditions identified in PIA

Section instructions, a glossary at Appendix 1, and explanatory notes at Appendix 2, provide more detail on completing the DATA OUT PIA module. Tables are colour-coded (as above) to indicate who should complete them.

JOINT BORDER ANALYTICS

Single-Agency Privacy Impact Assessment – DATA OUT module

Complete a separate DATA OUT module for each external dataset required for the activity.

1. Activity Sign off

What's this for?	*This section captures Requesting Agency approval for the activity and also records that this PIA has been reviewed by the Requesting Agency's Privacy Officer or team. An activity cannot proceed until this section has been completed.*
Who should complete this?	*Requesting Agency approval must be **Chief Executive level or above**.*

Requesting Agency	**NZCS**
Activity approved by	**Privacy review by**
s 9(2)(g)(ii) OIA [redacted] **Date: 27 May 2022** **Approval:** [redacted]	s 9(2)(g)(ii) OIA [redacted] **Date: 19 July 2022** **Approval:**

JOINT BORDER ANALYTICS

JBAC
PIA reviewed by
s 9(2)(g)(ii) OIA [redacted] **Date: 17 May 2022** **Approval:** [redacted]

2. Governance and contact information

What's this for?	*This section records which border agency initiated the analytics 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 Requesting Agency.*

Date PIA commenced	16 May 2022
JBAC contact person for this activity	s 9(2)(g)(ii) OIA [redacted]
Requesting Agency	NZCS - Intelligence

JOINT BORDER ANALYTICS

Activity contact person for Requesting Agency	s 9(2)(g)(ii) OIA [redacted]
Privacy/legal representative for Requesting Agency	

3. Overview of the activity

What's this for?	*This section explains the analytics activity, for the purpose of assisting the Requesting Agency to make the output assessment.*
Who should complete this?	***JBAC** will complete this section on behalf of the Requesting Agency.*

1. What is the name of this activity?	Counter Terrorism s 6(c) OIA [redacted]	
2. Briefly describe the activity, including the problem/s it is seeking to address	s 6(c) OIA [redacted]	
3. How does this activity support the Requesting Agency's lawful purposes and deliver public benefit? [2]	NZCS	[redacted]

	s 6(c) OIA [redacted]

4. What existing datasets are required for this activity?	Dataset	Data elements	Time period	Relevance to activity
	s 6(c) OIA [redacted]			

5. What external datasets are required for this activity?	Dataset	Data elements	Source	Time period	Relevance to activity
	s 6(c) OIA [redacted]				
6. Relevant attached documents					

JOINT BORDER ANALYTICS

4. Identifiable intelligence output assessment

What's this for?	*This section assesses the lawfulness, fairness, proportionality and necessity of identifiable intelligence outputs.*
Who should complete this?	***JBAC** will complete the overview of the outputs, as the analytics SME. The **Requesting Agency** must complete this assessment for each output to ensure that they are satisfied it is lawful etc.*

1. Briefly describe the output	s 6(c) OIA [redacted]
2. What personal information will the output include?	
3. What business unit(s) within the Requesting Agency will receive or use the output?	
4. What security classifications or handling caveats will be applied to this output? [6]	
5. What steps has JBAC taken to ensure the data used to generate the output is accurate and up-to-date? [7]	
6. Briefly describe the algorithm used to generate the output, including the determinative data fields [8]	
7. What steps have been taken to ensure the datasets are free from unwanted bias? [9]	

	s 6(c) OIA
8. What steps have been taken to ensure the analytics or outputs are not unlawfully discriminatory? [10]	

1. Are you satisfied that you have a lawful basis to use the personal information contained in this output? *IPP 10* **[3]**	☐ No, we do not think there is a lawful basis		**Action required**
	☒ Our enabling legislation	See Question 3 for C&E Act references. NZCS may use information provided to and held NZCS for "any lawful purpose relation to, or connected with, the carrying out of any function of Customs under the C&E Act or any other enactment." Here the information held by NZCS will be used to further Customs' function of risk assessment at the border s 6(c) OIA	Proceed
	☒ Principle 10(c)(i) – maintenance of the law **[4]**	See Question 3 s 6(c) OIA	Proceed
	☐ Principle 10(d) – serious threat **[5]**		Proceed
	☐ Other		Proceed
2. Are you satisfied that the output is relevant to your lawful purposes? [11]	☐ Not sure, we need more information		**Action required**
	☐ No, it is not relevant		**Action required**
	☒ Yes, it is relevant		Proceed

3. Have reasonable steps been taken to ensure the dataset is accurate and up-to-date before it is used? *IPP 8*	☒ Yes, reasonable steps have been taken	The model is only utilising data s 6(c) OIA [redacted] to ensure we are using the most up to date data.	Proceed
	☐ No, additional steps may be required		**Action required**
4. Are you satisfied that this output is proportionate to the problem it is intended to address? [12]	☐ Not sure, we need more information		**Action required**
	☐ No, it is not proportional		**Action required**
	☒ Yes, it is proportional	Controls have been put in place to ensure that only relevant data is returned s 6(c) OIA [redacted]	Proceed
5. Are you satisfied that sufficient steps are in place to protect against unwanted bias or unlawful discrimination? [9] [10]	☐ Not sure, we need more information		**Action required**
	☐ No, we are not satisfied		**Action required**
	☒ Yes, we are satisfied	See Question 7 – algorithm design has been done to remove any bias s 6(c) OIA [redacted]	Proceed
6. Are you satisfied that the output will be appropriately classified or caveated? [6]	☐ No, we are not satisfied		**Action required**
	☒ Yes, we are satisfied	The information contained in this report is classified as RESTRICTED and should not be disseminated further or released without prior permission of the CCO/Manager JBA	Proceed
7. Are you satisfied that the business unit(s) receiving the output have the necessary security clearance?	☐ No, we are not satisfied		**Action required**
	☒ Yes, we are satisfied	Outputs will not be above RESTRICTED and Intelligence staff are all cleared to at least RESTRICTED.	Proceed
	☐ No, we do not		**Action required**

8. Do you have processes in place to ensure that this output is validated before being relied upon to take adverse actions?	☒ Yes, we do	Output from the model does not automatically lead to an adverse action against any individual. Output will go to CT Intelligence staff for further assessment and validation using other data sources (e.g. CUSMOD) before any decisions about further actions are made. s 6(c) OIA [redacted]	Proceed
9. Do you have processes in place to ensure that individuals can challenge any adverse actions taken on the basis of this output?	☐ No, we do not		**Action required**
	☒ Yes, we do	Normal OIA processes will allow individuals to request any information Customs has on them, which could then be used as a basis for challenging adverse actions. As set out in the answer to question 8, output from the model will not in itself trigger an adverse action – further assessment from CT Intelligence is still required.	Proceed
10. Privacy/Legal team comments	NZCS Legal comments 11 July 2022 s 9(2)(h) OIA [redacted]		
11. Can the output proceed as intended?	☒ **Yes** - Approved by: s 9(2)(g)(ii) OIA [redacted]		
	☐ **Yes, but**:	☐ We need to take steps to ensure data accuracy [populate R3] ☐ We need to establish steps to protect against bias [populate R4] ☐ We need to ensure the correct security clearances are in place for an output recipient [populate R8] ☐ The output needs to be correctly classified or caveated [populate R9]	

		☐ We need to establish a process to validate the output [populate R6] ☐ We need to establish a process for individuals to challenge adverse actions [populate R7]
	☐ **No, because**:	☐ We have no lawful basis to use [populate R1] ☐ The output may not be relevant to our lawful purposes [populate R2] ☐ The output may not be proportionate [populate R5] ☐ The output may be biased or unlawfully discriminatory [populate R10] ☐ Other [populate other]

5. Privacy risks, mitigations and actions

What's this for?	*This section captures any risks generated by the outcome of section 3. JBA or the Requesting Agency can also add more risks and mitigations here.*
Who should complete this?	***JBAC** will complete this section on behalf of the Requesting Agency but the **Requesting Agency** may also add content as required.*

Risk	Mitigation/Action	Responsible	Date complete
R1 ☐ The Requesting Agency has no lawful basis to use personal information		N/A	
R2 ☐ The output is not relevant to the Requesting Agency's lawful purposes		N/A	
R3 ☐ We need to take steps to ensure data is accurate etc before generating the output		N/A	
R4 ☐ We need to take steps to protect against bias		N/A	
R5 ☐ The output is not proportionate		N/A	

R6 ☐ The Requesting Agency needs to establish a process to validate the output		N/A	
R7 ☐ The Requesting Agency needs to establish a process for individuals to challenge adverse actions		N/A	
R8 ☐ The Requesting Agency needs to ensure the correct security clearances are in place		N/A	
R9 ☐ The output has not been correctly classified or caveated		N/A	
R10 ☐ The output may be biased or unlawfully discriminatory		N/A	
☐ Other		N/A	

JOINT BORDER ANALYTICS

Appendix 1: Glossary

This	Means
Activity	an agreed and authorised (by the Requesting Agency) use of data analytics to produce a set of outputs that may include analytics models, forecasts or identifiable intelligence outputs.
Adverse action	any action that may adversely affect the rights, benefits, privileges, obligations, or interests of any specific individual; including any decision: 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: ii. to investigate the possible commission of an offence: 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.
Analytics forecasts	forecasts designed to look forward at possible future patterns of border risk using historical information. These products contain no personal information.
Analytics models	models that identify a class 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).
Border agencies	DIA, DOC, MBIE, MPI or NZCS.
CRISP-DM	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.
Data analytics	the discovery, interpretation, and communication of meaningful patterns in data.
Data exploration	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.
Data refinement	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.

Dataset	a distinct category of data held by the Requesting Agency, by a third-party agency or that is publicly available. Each dataset will include data fields that may relate to identifiable individuals.
DIA	Department of Internal Affairs.
DOC	Department of Conservation.
Enabling legislation	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.
Identifiable intelligence outputs	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.
JBAC	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.
MBIE	Ministry of Business, Innovation and Employment, which includes Immigration New Zealand.
MPI	Ministry for Primary Industries.
NZCS	New Zealand Customs Service.
Personal information	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.
Requesting Agency	the border agency that has initiated the activity, will provide the platform within which the activity will be completed, and will be the sole recipient of any identifiable intelligence outputs.
Unlawful discrimination	discrimination based on any grounds prohibited by the Human Rights Act 1993, including sex, martial status, religious belief, colour, race, ethnic origin, disability, age, political opinion, and sexual orientation.

JOINT BORDER ANALYTICS

Appendix 2: 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 collecting 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 Requesting Agency's 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 Requesting Agency consider, and can demonstrate, positive **public benefits** from collecting, analysing and using personal information. A clear link to Requesting Agency's lawful purposes (as set out in its enabling legislation) is also required to ensure that an activity is legitimate and necessary.

[3] The burden of establishing that an exception applies to permit a collection or use of personal information rests with the Requesting Agency seeking to rely on it. The Requesting Agency may seek further clarity from JBAC where this is required in order to establish whether an exception applies.

[4] 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.

[5] 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.

[6] **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.

[7] **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).

[8] **Algorithmic transparency** is an important element of fairness and due process. JBAC must be able to explain to the Requesting Agency 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.

[9] JBAC should assist the Requesting Agency 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.

[10] 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.

[11] The Requesting Agency 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.

[12] The Requesting Agency 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.