



ABS RESPONSE

Criminal Justice Data Asset Privacy Impact Assessment

May 2025



CONTENTS

INTRODUCTION	3
Project Background	3
RESPONSE TO RECOMMENDATIONS	4
Recommendation 1: Re-identification risk management	4
ABS Response: Agreed	4
Recommendation 2: Further privacy risk assessments	4
ABS Response: Agreed	4
Recommendation 3: Periodic reviews	4
ABS Response: Agreed	4
Recommendation 4: Data sharing agreements with source data custodians	5
ABS Response: Agreed	5
Recommendation 5: Governance of Indigenous Data	5
ABS Response: Agreed	5
Recommendation 6: Transparency and notification	5
ABS Response: Agreed	5
Recommendation 7: Data quality and statistical linkage key	6
ABS Response: Agreed	6

INTRODUCTION

Project Background

The Australian Bureau of Statistics' (ABS) National Crime and Justice Data Linkage Project (Project) aims to develop a longitudinal national criminal justice data asset, known as the Criminal Justice Data Asset (CJDA).

The Project was initiated out of the Council of Australian Governments' *Prison to Work Report* (2016), which noted that there were 'data gaps and a patchy evidence base for what works' to improve outcomes for prisoners and ex-prisoners.¹ The *Prison to Work Report* made a number of recommendations to address these shortcomings, including that:

- State and Territory governments work with the Commonwealth to 'share essential de-identified criminal justice data (including corrections, courts, police and juvenile justice) to enable the quantifying of the flow of prisoners through the system';
- the Commonwealth and State and Territory governments work together to 'identify and remedy data gaps'; and
- the Commonwealth, together with State and Territory governments, 'conduct a project linking the data for persons moving through the child protection, justice, health, welfare and employment systems'.²

The aim of the CJDA is to enhance the suite of ABS crime and justice data collections to enable person-level linkage, forming a longitudinal and enduring nationally linked up justice data asset available to approved users. The CJDA will link information about people that come into contact with the criminal justice sector using administrative data already provided to the ABS from the police, criminal courts and corrective services departments nationally – specifically, for the annual publications: [Recorded Crime – Offenders](#); [Criminal Courts, Australia](#) and [Prisoners in Australia](#).

De-identified data from the CJDA will be made available via the ABS DataLab to approved policy analysts and researchers to better understand aspects of criminal behaviour and provide opportunities to develop, monitor and evaluate criminal justice policies.

The ABS engaged an independent law firm; Clayton Utz³, to conduct a Privacy Impact Assessment (PIA) of the Project, specifically for the development of the CJDA. The PIA considers the privacy implications of integrating administrative criminal justice data. The PIA identifies and assesses privacy and secrecy compliance risks and makes recommendations for eliminating, reducing or managing those privacy and secrecy compliance risks.

The ABS with support from MinterEllison⁴, consulted with a range of stakeholders to inform the PIA. Clayton Utz produced the PIA Report with recommendations informed by the outcomes from the consultation sessions, summarised in the Consultation Report.

The PIA Report, Consultation Report and this response can be accessed via the [ABS website](#).

The ABS welcomes the findings and recommendations of the PIA. This document outlines the ABS response to the recommendations.

¹ Council of Australian Governments, *Prison to Work Report* (2016), pp 7, 48–53.

² *Prison to Work Report*, Finding 9.

³ Note that the PIA was commenced by MinterEllison and finalised by Clayton Utz.

⁴ See Footnote 3.

RESPONSE TO RECOMMENDATIONS

Recommendation 1: Re-identification risk management

We recommend that the ABS periodically review the efficacy of the measures that the ABS has in place to manage the risks of re-identification (including any changed or increased risks over time) in the context of the Project. These periodic reviews should consider:

- *the kind of information that is made available to researchers through the DataLab (and whether individuals may be identifiable due to unique or uncommon characteristics that enable identification;*
- *the kind of information that is permitted to be released from the DataLab; and*
- *the controls and safeguards that are in place in the DataLab, to manage re-identification risks.*

ABS Response: Agreed

Information for this Project will be made available to researchers under section 15 of the *Census and Statistics (Information Release and Access) Determination 2018* (C&S Determination) via the ABS DataLab (a secure analysis environment). Section 15 and the C&S Determination more broadly, does not permit the release of information in a manner that may enable the identification of a particular person.

The ABS periodically reviews risks of re-identification as part of overall ABS data confidentiality and data integration practices, which also includes assessment of type of information which will be made available through the DataLab. This Project will follow the same protocols.

Recommendation 2: Further privacy risk assessments

If there are any new or material changes to the information flows identified in Schedule 1, including:

- *the collection of additional types of personal information;*
- *additional or changed uses of personal information not identified in Schedule 1;*
- *the sharing of personal information with third parties not identified in Schedules 1 or 3; or*
- *as a result of changes to the Project and/or the way in which it is administered,*

a privacy threshold assessment and, if required, further assessment of privacy impacts and compliance risks, should be undertaken (which could be in the form of a supplementary PIA.

The assessment(s) should consider privacy impacts from both privacy law compliance and community expectations perspectives.

A further secrecy compliance assessment should also be undertaken, as necessary and to the extent that there are any new or material changes to the protected information flows identified in Schedule 1.

ABS Response: Agreed

As part of standard ABS data integration process, which this Project adheres to, privacy threshold assessments are conducted when there are new or significant changes to the project or processes. The ABS must protect information and data collected under the *Census and Statistics Act 1905* (C&S Act) in accordance with the secrecy provisions within the C&S Act.

Recommendation 3: Periodic reviews

We recommend that the ABS periodically review the operation of the Project to ensure:

- *methods for handling personal information remain appropriate, and align with community expectations;*
- *ongoing APP compliance; and*
- *opportunities to refine data handling practices and maximise privacy protection can be identified and implemented.*

ABS Response: Agreed

As per the ABS Response to Recommendation 1, ABS data integration practices for all DataLab projects

include periodic review of data handling practices and compliance.

Recommendation 4: Data sharing agreements with source data custodians

We recommend ensuring that the terms of each Memorandum of Understanding (MOU) - or other form of data sharing agreement, between the ABS and each source data custodian address the following matters:

- *the data that the source data custodian will provide to the ABS;*
- *the purpose for which the source data custodian will provide the relevant data to the ABS, and the purposes for which the ABS may use and disclose that data;*
- *the legal authority under which each party will collect, use and disclose the relevant data;*
- *arrangements and requirements relating to the secure transfer/sharing and storage of data;*
- *each party's obligations with respect to:*
 - *compliance with applicable privacy laws, namely:*
 - *for the ABS – the Commonwealth Privacy Act and APPs; and*
 - *for data custodians – the Commonwealth Privacy Act and APPs, or an equivalent privacy law that binds the data custodian in their jurisdiction;*
 - *compliance with other relevant legislation that may apply to the data provided by the data custodian (e.g. secrecy provisions in legislation); and*
 - *where necessary, obtaining their own legal advice and undertaking their own PIAs (or other form of privacy risk assessments) prior to sharing any data;*
- *obligations and processes relating to the notification and handling of data breaches and privacy complaints.*

ABS Response: Agreed

As per ABS standard processes, the ABS will develop and enter into MOUs (or other form of data sharing agreements) with each source data custodian for the development of the CJDA. These will outline clearly:

- the purpose of the Project and CJDA;
- specifications for the data, including secure transfer arrangements;
- the legal authority for data collection, disclosure and use as well as any other relevant obligations; and
- processes relating to handling of data breaches and privacy complaints.

Recommendation 5: Governance of Indigenous Data

We recommend that the ABS embed and operationalise best practice for the governance of Aboriginal and Torres Strait Islander data into the CJDA. These principles are outlined in the National Indigenous Australians Agency's [Framework for Governance of Indigenous Data](#).

ABS Response: Agreed

In alignment with National Indigenous Australians Agency's [Framework for Governance of Indigenous Data](#), over the next seven years the ABS will be committing and embedding the principles of the Framework into respective ABS statistical projects and collections, which include the CJDA.

The Framework was co-designed with Aboriginal and Torres Strait Islander representatives for the purpose of providing 'Aboriginal and Torres Strait Islander people greater agency over how their data are governed within the Australian Public Service so government held data better reflects their priorities and aspirations'.

Recommendation 6: Transparency and notification

We recommend that the ABS liaise with source data custodians to develop a strategy that supports transparency around the use of individual data for statistical purposes, including data integration. This strategy should aim to ensure that relevant individuals are informed about how their data is being collected and used, the purposes of data integration, and the measures in place to protect their privacy.

ABS Response: Agreed

The ABS supports transparency and encouraging the awareness of relevant individuals of the disclosure of their personal information.

The ABS will develop a communication strategy with source data custodians to encourage and improve their notice of the collection and use of data from individuals that they interact with as part of their operational services. However, there are practical limitations when using administrative by-product data from operational systems.

For the ABS administrative publications used in this Project, the ABS has tabled these to Parliament and releases the publications annually on the ABS website, supporting transparency and notification of the use of individual data for statistical purposes.

Recommendation 7: Data quality and statistical linkage key

We recommend that the ABS periodically review data quality, including the linkage methodology, to ensure that the data is fit for purpose for the Project.

ABS Response: Agreed

As per the ABS Response to Recommendation 1, ABS data integration practices include periodic review of data quality and linkage methodology. Specific for this Project, there will be a review of data quality (including linkage methodology) at the completion of the inaugural production process.



www.abs.gov.au