Australian Bureau of Statistics

PRIVACY IMPACT ASSESSMENT

ACT Government's Justice and Community Safety Directorate - Reducing Recidivism by 25% by 2025 Plan

May 2025

Contents

PART 1. INTRODUCTION

1.1 Background

The Australian Capital Territory (ACT) Government's Justice and Community Safety Directorate (ACT JACS) has requested that the Australian Bureau of Statistics (ABS) link together administrative datasets from three ACT justice sectors (Police, Criminal Courts and Corrective Services - Prisoners) to help inform the evaluation of the ACT's Reducing Recidivism by 25% by 2025 Plan. For this project, the ACT Government are working with Australian National University's (ANU) Centre for Social Research and Methods as part of the Reducing Recidivism Research Collaboration. The ABS will be facilitating the data linkage and ANU researcher access to the integrated data for the development of recidivism outcome indicators.

The justice administrative datasets for this project are by-products from the ACT departments responsible for police, criminal courts and corrective services. These data are derived from administrative records held by these agencies in relation to people who come into contact with the criminal justice system. The data were provided in electronic format and received through the ABS Informatica portal.

The datasets are collected by the ABS under the *Census and Statistics Act 1905* for the compilation of national crime and justice statistics. Inter-Governmental Agreements are in place with the ACT which outline arrangements for the data provision for national crime and justice statistics, and direct agreement has been obtained from data custodians to cover the data integration activities of this project. The *Information Privacy Act 2014* (ACT) permits information collected by an ACT public sector law enforcement body for the purposes of its functions/activities to be disclosed for secondary purposes (e.g. statistical publications) where the information sharing is legally required or authorised by law.

National Crime and Justice Data Linkage Project & Criminal Justice Data Asset

In parallel, the ABS is developing the National Crime and Justice Data Linkage Project (NCJDLP). This ACT JACS project utilises similar datasets and linkage methodologies as the NCJDLP project. The aim of the NCJDLP is to enhance the suite of national crime and justice data collections to enable person-level data linkage, forming a longitudinal and enduring nationally linked up justice data asset, known as the *Criminal Justice Data Asset* (CJDA). The CJDA will only be used for approved research and policy purposes, allowing for analysis of how persons move through and interact with the criminal justice system between jurisdictions and/or across time. The NCJDLP and CJDA have been subject to a separate Privacy Impact Assessment (PIA).

1.2 Purpose, scope, and approach

1.2.1 Purpose

The purpose of this PIA is to:

- Consider the potential privacy impacts on people whose personal information has been provided to the ABS and whose de-identified information will be made available to authorised researchers for this project;
- Identify privacy risks in relation to the Australian Privacy Principles (APPs) and community expectations; and
- Identify, assess, and outline risk mitigation strategies to manage privacy impacts.

1.2.2 Scope

This PIA covers the one-off linkage of the three ACT criminal justice administrative datasets (ACT data) and ANU researcher access to this linked data for the purpose of developing recidivism indicators to inform the ACT JACS Reducing Recidivism by 25% by 2025 Plan. The PIA will summarise the data flows and processes involved, and the protections for managing personal and sensitive information, as well as addressing community expectations around the project. The PIA also assesses the overall compliance of this project with APPs.

This project uses standard ABS data integration processes and infrastructure as used for the Person Level Integrated Data Asset (PLIDA). This PIA builds on previous privacy work for these processes and

infrastructure including previous PLIDA PIA Updates and the ABS Cloud DataLab PIA for standard ABS provision of researcher access (within the ABS DataLab).

The NCJDLP and CJDA are not in scope of this Privacy Impact Assessment.

1.2.3 Approach

The ABS followed the Office for Australian Information Commissioner's (OAIC) Guide to undertaking privacy impact assessments in completing this PIA. This included:

- Undertaking a Privacy Threshold Assessment (PTA) to determine the need for the PIA based on a shortlist of risk criteria;
- Mapping information flows;
- Identifying and consulting with stakeholders;
- Privacy impact analysis and compliance check;
- Privacy management — addressing risks; and
- Recommendations.

1.3 Personal and Sensitive Information

1.3.1 Personal Information

The *Privacy Act 1988 (Cth)* defines personal information as *"…information or an opinion about an identified individual, or an individual who is reasonably identifiable…*"

The *Information Privacy Act 2014 (ACT)* also defines personal information similarly.

Use of Personal Information in this project

The datasets involved in this project are based off the annual ACT extracts from 2015-16 to 2023-24 for the following ABS administrative collections:

- *Recorded Crime – Offenders*
- *Criminal Courts, Australia*
- *Prisoners in Australia*

These datasets contain identified personal information to support analyses and development of recidivism indicators of persons that interact with the ACT criminal justice system. Personal identifiers include parts of name, date of birth and sex, to enable linking between datasets as described in Part 2 of this PIA. The data will be handled in line with ABS security protocols as outlined in Part 2.

Previous PLIDA PIA Updates address the use of identifying personal information in detail, and the same processes (e.g. Separation principle, Five Safes Framework) and infrastructures (e.g. Secure ABS IT Environment, Secure ABS Data Integration Environment) will apply to this project:

"Direct identifiers are stored separately from other information in PLIDA in accordance with the separation principle. This other information may, in some circumstances, be considered personal information even when it is separated from direct identifiers as it may enable the re-identification of an individual (e.g. through the combination of data items). Access to personal information in PLIDA is strictly controlled and limited to a small team of ABS staff.

The PLIDA data that the ABS makes available for authorised researchers in the secure ABS DataLab does not include personal information as it is provided in a manner that is not likely to enable the identification of an individual (and therefore meets the requirements to be "de-identified" under the Privacy Act 1988 (Cth). The ABS uses the Five Safes Framework to manage disclosure risks associated with providing access to de-identified PLIDA data."

1.3.2 Sensitive Information

The *Privacy Act 1988 (Cth)* defines 'sensitive data' as information or an opinion about an individual's:

- racial or ethnic origin
- political opinions
- health information

- religious affiliation
- sexuality
- criminal record.

The *Information Privacy Act 2014* (ACT) also defines sensitive information similarly.

Use of Sensitive Information in this project

The ACT data used in this project contains sensitive information including racial and ethnic origin, criminal record, and interaction with the criminal justice system. The ABS applies the following principles for managing sensitive data:

- Only collecting and sharing the minimum amount of personal information required for the purposes of the project (the minimisation principle);
- Using categorised or derived indicators for sensitive data items where feasible, unless sensitive data items in their original form are required for statistical or analytical purposes; and
- Project proposals requiring specific justification for requesting sensitive data items.

1.4 Legislation and Policies

The *Information Privacy Act 2014* (ACT) regulates how personal information is handled by ACT public sector agencies. This Act includes a set of *Territory Privacy Principles (TPP)*, which cover the collection, use, storage and disclosure of personal information, and an individual's access to and correction of that information. Specifically, TPP 3.4(d) applies to information collected by an enforcement body where the information is directly related to an agency's functions/activities. Information has been disclosed to the ABS in accordance with TPP 6.2, which states that information can be disclosed for secondary purposes (e.g. statistical publications) if the information sharing is legally required or authorised by law. The legal requirement is via the ABS *Census and Statistics Act 1905.*

The ABS is authorised to request the collection of data on a range of matters under section 10(3) of the *Census and Statistics Act 1905* . This Act requires the ABS to compile and analyse such information, which may include linkage, and to publish and disseminate results of such compilations and analyses, while maintaining the confidentiality of the information provided. Section 15 of the *Census and Statistics (Information Release and Access) Determination 2018* permits the ABS to disclose unit record information to researchers for statistical and research purposes, provided all direct identifiers have been removed and the information is disclosed in a manner that is not likely to enable the identification of a particular individual. In addition, the ABS will seek agreement from a data provider that statistical results outputted from the ABS environment may be done in such a manner that may enable the indirect identification of that particular data provider.

ABS data integration practices comply with the High Level Principles for Data Integration Involving Commonwealth Data for Statistical and Research Purposes. The use of personal and sensitive information is governed by the Five Safes Framework to minimise disclosure risk.

As a Commonwealth organisation, the ABS is bound by the *Privacy Act 1988* including the Australian Privacy Principles (APPs). Compliance with the APPs is assessed in Part 3 of this PIA.

1.5 Addressing community expectations

While the collection, use or disclosure of personal information, including sensitive information, may be authorised by legislation, this does not necessarily mean it meets community expectations. A key privacy consideration is the right for individuals to be aware of how their personal information is being used. This PIA considers community attitudes and expectations regarding the project's privacy implications and risks to build and maintain public trust.

Public trust is critical to the ABS' reputation and to people's willingness to participate in ABS and government projects. Important steps in building public trust in this project include:

- Listing the project on the ABS Data Integration Project Register as well as publishing this PIA for transparency;
- Consultation with stakeholders;
- Ethics consideration; and

- Application of security controls detailed in Parts 2 and 3.

1.5.1 ACT Government Consultation

ACT JACS undertook consultations with several organisations and groups within the ACT Government to understand their views on the data linkage work planned for the Reducing Recidivism by 25% by 2025 evaluation. These included:

- Chief Minister, Treasury and Economic Development Directorate;
- ACT Justice and Community Safety Directorate Chief Information Officer and Executive Branch;
- ACT Directorate and Agency Heads, Reducing Recidivism Executive Coordination Group;
- ACT Policing;
- ACT Courts;
- ACT Corrective Services; and
- ACT Justice and Community Safety First Nations Justice Branch.

Overall, no serious privacy risks with the project were identified by the participating stakeholders. It was noted that the ABS was seen to have strong safeguards and controls in place to protect confidentiality. It was recognised that similar ACT Government datasets (de-identified) have been provided to the ABS previously without issue and that the ACT Government had been involved in extensive data linkage projects previously. Further, there were discussions around how only aggregate outputs would be released publicly, and that these outputs would be vetted to ensure compliance with confidentiality requirements, providing further security.

The consultations also noted the importance of this research, and it was recognised as an important way to gain insights, given the lack of data available currently around relationships and systemic trends within the criminal justice system. Additionally, it was noted that there was the potential for analysis to be undertaken in relation to several priority cohorts (where appropriate), including women and Aboriginal and Torres Strait Islander people, in relation to a range of measures, including the rate and seriousness of reoffending.

The ACT JACS First Nations Justice Branch did raise a potential issue around data quality relating to Indigenous Status reporting, which is a data limitation that will need to be noted and assessed as part of any resulting analysis.

1.5.2 Aboriginal and Torres Strait Islander Consultation

For Aboriginal and Torres Strait Islander consultation specifically, the ACT JACS and ANU noted the existence of the Reducing Recidivism Research Advisory Committee (the Committee) which oversees the ANU's broader research into reducing recidivism. The Committee includes two First Nation representatives as well as a First Nation Governance Committee and was established to provide oversight and governance of all projects that fall under the Reducing Recidivism Research Collaboration. This committee has considered Aboriginal and Torres Strait Islander perspectives and the impact of this project on the Aboriginal and Torres Strait Islander community. The Committee will also help inform any future policy development that results from this research.

In line with ABS consultation protocols, the ABS undertook further consultation with an ACT Aboriginal and Torres Strait Islander representative who works within the ACT justice sector for a non-profit organisation. This organisation aims to contribute to the broader social wellbeing of Aboriginal and Torres Strait Islander people. Again, no data security or community concerns were noted with the project. There was discussion around understanding the narrative of any resulting analysis/data and to ensure that it would be honouring First Nation people, which would build on strengths and not deficit reporting. The ABS noted that they would recommend that ACT JACS and the ANU further consult with similar representatives to ensure that resulting analysis/outputs and narrative are appropriate before they are publicly released.

1.5.3 Ethics

The ANU have conducted their own ethics process for this project and research work. Ethics approval was obtained through the ANU's Human Research Ethics Committee (HREC). The ANU HREC reviews proposed research projects involving human subjects that fall within the jurisdiction of the ANU, and approves research projects that meet the requirements of the National Statement on Ethical Conduct in

Human Research and are ethically acceptable. As this project may include Aboriginal and Torres Strait Islander research, the ANU HREC follows the *AIATSIS Code of Ethics for Aboriginal and Torres Strait Islander Research*.

PART 2. DATA USE AND INFORMATION FLOWS

2.1 Governance

The ABS and ACT JACS have negotiated direct agreements with the data custodians to permit the usage of their data by the ABS for this data integration purpose. As noted, the ACT data will be linked as a one-off stand-alone project.

As an Accredited Integrating Authority, the ABS is responsible for receiving, storing, and linking data, assembling extracts of integrated data, and providing access to de-identified data to authorised researchers to analyse.

All data integration activity will be performed in line with ABS functional separation principles and conducted in the Secure ABS Data Integration Environment. ABS use of personal information is governed by the Five Safes Framework, as outlined in previous PLIDA PIA Updates.

Data used in this project was collected by the ACT justice agencies under the *Information Privacy Act 2014* (ACT) which regulates how personal information is handled by ACT public sector agencies. This Act includes a set of *Territory Privacy Principles (TPP)*, which cover the collection, use, storage and disclosure of personal information, and an individual's access to and correction of that information. Data was disclosed to the ABS under TPP 6.2, which permits disclosure for secondary purposes if the information sharing is legally required or authorised by law. Data was collected by the ABS under the *Census and Statistics Act 1905*.

2.2 Integration of the data

This project adheres to the Separation Principle, which has been achieved through applying 'functional separation' so that ABS staff working on the project have different functions, or roles, and access to data depends on what is necessary for each role. The roles for this project are librarian (prepares data for linkage), linker (links data), assembler (assembles extracts and other products for analysis), and analyst (analyses integrated data extracts or products for policy analysis, research, or statistical purposes). Allocating people to these roles ensures each person cannot access personal identifiers and analyse information at the same time.

Personal identifying information (such as date of birth) will be separated from the analytical information by access-controlled files for the datasets.

2.3 Analysis

Analysis will be performed by approved ANU researchers in the secure ABS DataLab Environment, adhering to the Five Safes Framework. As part of the 'Safe data' requirement, direct identifiers will be removed from linked analytical data and further statistical disclosure controls may be applied. Only approved ANU researchers who have undergone ABS DataLab training will have access to the linked analytical data in the ABS DataLab. As part of the 'Safe people' requirement, approved researchers are required to have a legally binding undertaking to maintain data confidentiality.

2.4 Research outputs

As standard practice, the 'Safe output' test of the Five Safes Framework will be applied to ensure that no data that can enable the identification of an individual will be released from the ABS DataLab, consistent with ABS obligations under the *Census and Statistics Act 1905*.

2.5 Retention of information

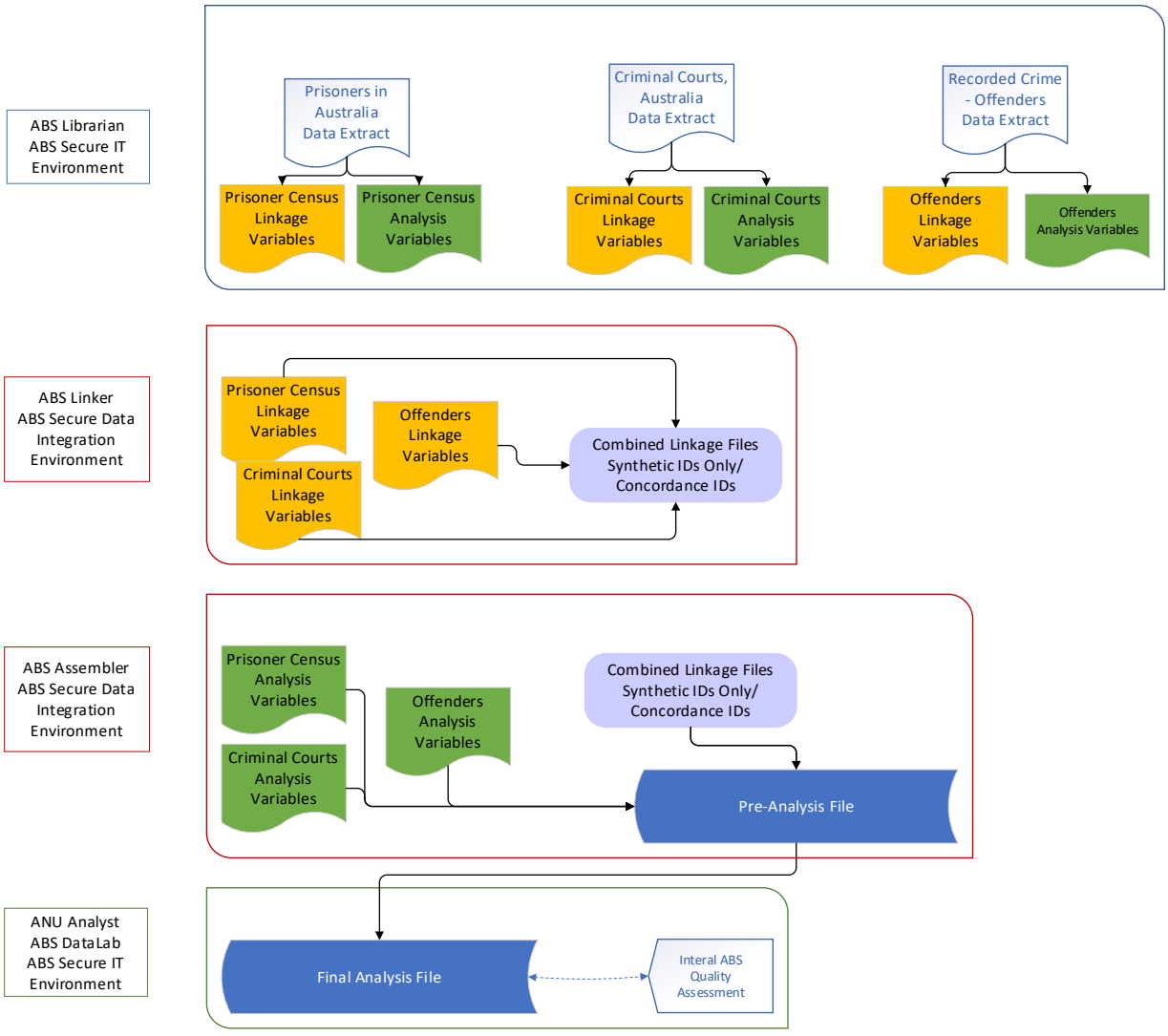
The ABS recognises that retaining data when it is no longer needed presents security risks. It is intended that the identifying information will be destroyed at the conclusion of project, subject to the ABS Data Integration Policy and the ABS Retention of Personal Identifiers for Statistical Purposes Policy. The analytical data will be destroyed when the ABS is no longer required to retain it, in line with ABS record keeping obligations under the *Archives Act 1983*.

2.6 Map of Information Flow

See diagram below for a basic map of information flows for this project within the ABS environments. This project utilises similar processes as the PLIDA Information Flow. Please refer to previous PLIDA PIA Updates.

1. The ABS Librarian will clean raw data extracts from each of the ACT justice datasets. These files will be transferred to the ABS Linker.
2. The ABS Linker role creates the Combined Linkage File using the linkage variables from each of the datasets. This shows the correspondence between the datasets through linkage IDs. From this point forward, files contain no identifying information, only analysis variables and non-identifying IDs.
3. The ABS Assembler role creates a linked pre-analysis file using the initial linkage concordance received from the Linker role, as well as the files containing analysis variables.
4. The ABS Assembler removes the linkage IDs and assigns randomly generated synthetic IDs to create the final analysis file. The file may be subject to further treatments before the final file (or a subset thereof) can then be accessed by the Analyst role in the ABS DataLab.
5. The approved ANU Analyst will have access to the de-identified final analysis file in the ABS DataLab environment. Analysts must go through a vetting process, complete mandatory training and sign deeds of undertaking to maintain data confidentiality prior to being onboarded to the DataLab. All ABS DataLab analysis is monitored to ensure that only approved analysis and outputs are created.
6. Any resulting outputs for release from DataLab are vetted by ABS staff as per standard DataLab arrangements, to ensure confidentiality requirements are met.

Diagram – Map of Information Flows



Part 3. AUSTRALIAN PRIVACY PRINCIPLES

APP 1 – open and transparent management of personal information

APP 1 requires that an entity manages personal information in an open and transparent way, including having a clear, up to date privacy policy that is publicly available. APP 1 also requires that an APP entity takes reasonable steps to implement practices, procedures and systems that ensure it complies with the APPs.

Compliant

The key external facing policies for ABS management of personal information - ABS Privacy Policy for Statistical Information - are compliant with APP 1.

The ABS Privacy Policy for Statistical Information describes how the ABS handles personal information that is collected for producing official statistics. This includes information in datasets like the ACT JACS datasets that will be linked as part of this project. The Policy outlines:

- the kinds of personal information collected and held by the ABS
- how we collect data and keep personal information safe
- how personal information is used
- accessing and correcting personal information
- our legislative responsibilities
- how privacy complaints and enquiries can be raised and managed.

APP 2 – anonymity and pseudonymity

APP 2 requires that APP entities give individuals the option of not identifying themselves, or of using a pseudonym. Limited exceptions apply.

Compliant

Data used in this project is compliant with APP 2 due to exceptions to anonymity and pseudonymity requirements where:

- "the APP entity is required or authorised under Australian law to do so, or
- if it is impractical for the APP entity to deal with individuals who have not identified themselves or who have used a pseudonym."

It is not practicable for the ABS to deal with individuals who have not identified themselves or who have used a pseudonym as the ABS requires identified information to perform data linkage. To protect against the risk of a data breach or disclosure risk, names and other identifying information are held separate to the analytical information in keeping with the functional separation principles.

APP 3 – collection of solicited personal information

APP3 covers the collection of both personal and sensitive information, the means of collections, and solicited personal information.

Compliant

Personal information other than sensitive information

APP 3.1 and 3.2 require that any personal information collected by an agency or organisation must be reasonably necessary for one or more of the collection APP entity's functions or activities.

As required by APP 3.1, all data collected by ABS for this project is reasonably necessary for the ABS to perform its function as an Accredited Integrating Authority. Personal information, such as parts of name, date of birth and sex, are needed to link between the ACT datasets to facilitate analysis required for this project. The collected data are covered in the prescribed matters described in regulation 13 of the *Census and Statistics Regulation 2016*.

Sensitive information

APP 3.3 specifies that sensitive information about an individual must not be collected by an APP entity unless:

a) the individual consents to the collection of information and:
    i. The information is reasonably necessary for, or directly related to, one or more of the agency's functions or activities; or
    ii. The information is reasonably necessary for one or more of the organisation's functions or activities; or
b) subclause 3.4 applies in relation to the information.

APP 3.4 covers examples where sensitive information may be collected. Subclause 3.4(a) outlines that sensitive information may be collected if the collection is required, authorised by, or falls under an Australian law.

As discussed in 1.4 Legislation and Policies, there are explicit Acts such as the *Census and Statistics Act 1905* which allows for sensitive data to be collected and used by the ABS for statistical purposes.

Means of collection

APP 3.5 requires that personal information may only be collected by lawful and fair means.

APP 3.6 specifies that personal information about an individual must be collected from the individual unless an exception applies:

a) the individual consents to the collection of the information from someone other than the individual; or
b) the entity is required or authorised by or under an Australian law to collect the information from someone other than the individual; or
c) it is unreasonable or impracticable for the entity to collect personal information only from the individual.

The ABS complies with APP 3.5 because it is authorised to collect, compile, analyse, and publish statistics under the *Australian Bureau of Statistics Act 1975* and the *Census and Statistics Act 1905*.

The ABS is also authorised by legislation and as an Accredited Integrating Authority to conduct projects that involve linking personal and sensitive data for statistical or research purposes. The ABS complies with APP 3.6 because, for this project, it would be unreasonable and impracticable for the ABS to collect this data from the individuals themselves.

The ACT data has been acquired from ACT government agencies and is covered by the *Information Privacy Act 2014* (ACT) which describes how personal information is handled by ACT public sector agencies. The Act allows for information collected by an enforcement body for the agency's functions/activities to be disclosed for secondary purposes.

APP 4 – dealing with unsolicited personal information

APP 4 requires that where an APP entity receives unsolicited personal information, it must determine whether it would have been permitted to collect information under APP 3. If APP 4.3 applies to the personal information, then the entity must destroy the information or ensure that it is de-identified as soon as possible, but only if it is lawful and reasonable to do so. If subclause 4.3 does not apply in relation to the personal information, APPs 5 to 13 will apply to that information.

Compliant

The ABS checks all received data for unsolicited information. Unsolicited data can be in two forms:

1. Variables supplied that were not requested
2. Data within approved variables that is not of the anticipated type (e.g. phone numbers in an address field).

Data checks are made in a secure access-controlled environment. Where unsolicited data is detected, the dataset is quarantined, and an assessment is conducted to determine the nature and extent of the issue. The data custodian is advised and provided with two options:

1. ABS securely deletes the original dataset and the provider resupplies a corrected version of the data
2. The provider agrees to ABS deleting the identified unsolicited data and continuing with the use of the sanitised file.

APP 5 – notification of the collection of personal information

APP 5 requires that where an APP entity collects personal information about an individual, it must take reasonable steps to notify the individual, or otherwise ensure the individual is aware of certain matters, which are outlined in APP 5.2.

Compliant

ACT data used in this project are collected by data custodians and then disclosed to the ABS. As listed in 1.3 Personal and Sensitive information, these data are already contributing to annual national crime and justice administrative collections which are published on the ABS website.

Previous PLIDA PIA Updates also include relevant recommendations that the ABS should:
'advocate with entities responsible for collection notices to enhance transparency about their disclosure of personal information to the ABS for PLIDA by taking responsible steps to update notices or otherwise make individuals aware of data use'
and
'continue to increase transparency about the collection and use of data, including personal information, for PLIDA in online materials'.

In line with this advice, the ABS will be transparent about the collection of personal information for this project by listing the project and datasets used on the ABS Data Integration Project Register.

APP 6 – use or disclosure of personal information

APP 6 requires that an APP entity only use or disclose personal information for the particular purpose for which it was collected (the 'primary purpose'), or for a secondary purpose if the person has consented or if an exception applies, such as where the secondary use or disclosure is required or authorised by or under an Australian law.

Compliant

Datasets were provided to the ABS under legislation authorising disclosure for select purposes (including the compilation of statistics). All information accessed in this project was collected by the ABS under the *Census and Statistics Act 1905* for the compilation, analysis and dissemination of results/statistics. A part of compilation is the integration of datasets as conducted in this project. *The Census and Statistics (Information Release and Access) Determination 2018* enables researchers to access data with all direct identifiers removed, in a way that does not enable an individual to be identified. See Part 2 for further discussion on use.

No personal information is disclosed as part of this project. Results will not be disclosed in a manner likely to enable the identification of a particular person, consistent with the requirements of the *Census and Statistics Act 1905*. See Part 2 for further discussion.

APP 7 – direct marketing

APP 7 requires that organisations must not use or disclose personal information for the purpose of direct marketing unless an exception applies, such as where the individual has consented.

Not Applicable

The ABS does not use or disclose information for the purpose of direct marketing.

APP 8 – cross-border disclosure of personal information

APP 8 requires that before an APP entity discloses personal information to an overseas recipient, the APP entity must take reasonable steps to ensure that the overseas recipient does not breach the APPs (other

than APP 1) in relation to the information, unless an exception applies, such as the individual has given informed consent.

Not Applicable

No personal information is disclosed by this project. ANU researchers are based in Australia and will access the information in the secure ABS DataLab environment.

APP 9 – adoption, use or disclosure of Government Related identifiers

APP 9 requires that certain classes of APP entities must not adopt, use, or disclose a person's government related identifier as its own identifier of the individual unless an exception applies.

Not Applicable

APP 10 – quality of personal information

APP 10 requires that an entity must take reasonable steps to ensure the personal information it collects is accurate, up to date, and complete.

Compliant

The ABS primarily relies on data custodians to provide accurate and up to date personal information. The ABS has extensive systems in place to ensure that personal information used in the project and all data linkage is of high quality. Research analysis and outputs are carried out by researchers and policy makers. While ABS officers review outputs for disclosure risk, the quality of the outputs produced in this project are reliant on the researchers who are carrying out the analyses.

Outputs of this project are confidential statistics and cannot be used to identify a particular person.

APP 11 – security of personal information

APP 11 requires that an APP entity must take reasonable steps to protect personal information it holds from misuse, interference, and loss, as well as unauthorised access, modification, or disclosure. It must also take reasonable steps to ensure personal information is destroyed or deidentified once it is no longer needed.

Compliant

The ABS has a robust framework of legislative, protective security, Information and Communication Technology (ICT), and data governance controls for protecting the privacy of individuals and ensuring data security. The *Census and Statistics Act 1905* prohibits the ABS from releasing information in a manner that is likely to enable the identification of an individual and makes it a criminal offence to breach security provisions. All personal information is handled in accordance with the *Privacy Act 1988* and the Australian Privacy Principles and abides by the High Level Principles for Data Integration Involving Commonwealth Data for Statistical and Research Purposes. All ABS staff that have access to the data are required to sign a lifelong Undertaking of Fidelity and Secrecy under the *Census and Statistics Act 1905*. All authorised researchers with access to the data are required to sign a legally binding undertaking that outlines a range of conditions of use, including the requirement to maintain the confidentiality of the information collected under the *Census and Statistics Act 1905*.

The ABS adheres to strong security protocols, such as functional separation, storage of data in a secure environment, and implementation of the Five Safes Framework. This project complies with the ABS data retention policy which ensures that the retention of information is managed in line with the *Census and Statistics Act 1905*, *Archives Act 1983*, and *Privacy Act 1988*.

All personal information collected by the ABS is protected in accordance with the Australian Government Protective Security Policy Framework and with the Australian Government records management regime. When no longer required, personal information is destroyed or deleted according to the National Archives of Australia's Administrative Functions Disposal Authority and our records authorities (2001/00000540 and 2007/00105946).

The ABS has strong security arrangements for all information technology systems used for the project. Key features include:

- Arrangements which conform with information technology security arrangements within the Australian Government Information Security Manual (ISM);
- Data integration for the project is carried out by a dedicated team in an isolated secure environment with no external connectivity;
- A Secure Internet gateway which is independently reviewed annually by the Australian Signals Directorate (ASD); and
- An ongoing program of security audits and systems accreditations.

For more information, see previous PLIDA PIA Updates and the ABS Cloud DataLab PIA, as this project uses these data integration systems and environments.

APP 12 – access to personal information; APP 13 – correction of personal information

APP 12 requires that an APP entity that holds personal information about an individual must give the individual access to that information on request unless an exemption applies.

APP 13 requires that an APP entity must take reasonable steps to correct personal information to ensure that, having regard to the purpose for which it is held, is accurate.

Compliant

While a person can apply to access or correct information held by the agency who collected it, it may not always be possible for the ABS to provide this access or make the corrections. This is because the relevant information may have been destroyed or personal identifiers deleted from the statistical information, which is done as soon as possible.

The ABS has policies and procedures in place for complaints and the correction of inaccurate data collected by the ABS under the *Census and Statistics Act 1905*. This includes data disclosed to the ABS by other data custodians for use in this project.

The ABS website includes current advice for accessing and correcting personal data collected under the *Census and Statistics Act 1905*:

- The *Freedom of Information Act 1982* (Schedule 2, Part II, Division 2) exempts the ABS from providing access to documents containing information collected under the *Census and Statistics Act 1905*.
- For personal information originally collected by other data custodians and shared with the ABS for data integration, each individual data custodian (and authorised entity) remains responsible for managing access requests relating to their own data holdings. They are also required to provide mechanisms for dealing with corrections and complaints, usually detailed in their respective privacy policies.

PART 4. CONCLUSION AND RECOMMENDATIONS

ABS standard data integration and microdata access procedures and protocols will be adhered to as part of this project, and they have been assessed as sufficient. ABS considers that sufficient protections are in place to protect the privacy of personal and sensitive information as part of linking administrative datasets within ACT justice sectors and providing ABS DataLab access to approved ANU researchers. Further, the ABS is satisfied with the community consultations considering this project and its privacy impacts to the community. While the ABS has determined the privacy risks are acceptable, the following recommendations are proposed to further enhance compliance and/or privacy protections for individuals.

Recommendation 1

As part of the ABS community consultations completed with ACT Aboriginal and Torres Strait Islander representatives, the ABS recommends that ACT JACS and ANU consult with similar groups/representatives to ensure that any resulting analysis/outputs and narrative are appropriate before they are released.

Recommendation 2

ABS to undertake wider consultation before the Criminal Justice Data Asset is released (which will include ACT datasets) and/or broader researcher access is provided to linked justice data.

As discussed in Part 1, the National Crime and Justice Data Linkage Project and Criminal Justice Data Asset have undergone an external Privacy Impact Assessment which includes consultation and consideration of privacy impacts of this type of data integration and use.

www.abs.gov.au