

Report: 13 November 2024
Australian Bureau of Statistics

CENSUS 2026 PRIVACY IMPACT ASSESSMENT (PHASE 2)



IIS Partners
INFORMATION INTEGRITY SOLUTIONS

Contents

1.	Executive summary	1
1.1	IIS's overall view	1
1.2	Summary of recommendations	2
2.	Introduction	4
2.1	Background	4
2.2	Scope of this assessment	4
2.3	Relevant legislation	5
2.4	Census privacy governance	6
2.5	Approach to this PIA	7
2.6	About this report	9
2.7	Personal information flows	9
3.	Enumeration including special dwelling enumeration	11
3.1	Changes expected in 2026	11
3.2	Personal and other information involved	11
3.3	APP analysis and other privacy risks	12
3.4	Summary	14
4.	Temporary workforce	15
4.1	Changes expected in 2026	15
4.2	Personal and other information involved	15
4.3	APP analysis and other privacy risks	16
4.4	Summary and recommendations	18
5.	Customer experience and engagement via social media	19
5.1	Changes expected in 2026	19
5.2	Personal and other information involved	20
5.3	APP analysis and other privacy risks	20
5.4	Summary	23
6.	Digital service and myGov Census pathway	24
6.1	Changes expected in 2026	24
6.2	Personal and other information involved	24
6.3	APP analysis and other privacy risks	25
6.4	Summary and recommendations	28
7.	Coverage and data quality	30
7.1	Changes expected in 2026	30
7.2	Personal and other information involved	30

7.3	APP analysis and other privacy risks	30
7.4	Summary	31
8.	Data design and WoAG Coding Capability	33
8.1	Changes expected in 2026	33
8.2	Personal and other information involved	33
8.3	Stakeholder feedback	35
8.4	APP analysis and other privacy risks	35
8.5	Summary and recommendations	38
9.	Use of administrative data	39
9.1	Changes expected in 2026	39
9.2	Personal and other information involved	39
9.3	Stakeholder feedback	40
9.4	APP analysis and other privacy risks	41
9.5	Summary and recommendations	49
10.	Business Locations Asset	53
10.1	Changes expected in 2026	53
10.2	Personal and other information involved	53
10.3	Stakeholder feedback	54
10.4	APP analysis and other privacy risks	54
10.5	Summary and recommendations	56
Appendix A.	Glossary	58
Appendix B.	Documents reviewed and meetings held	60
Appendix C.	List of external consultation stakeholders	65
Appendix D.	Overview of personal information flows	66

1. Executive summary

The Australian Bureau of Statistics (ABS) engaged IIS Partners (IIS) to conduct a privacy impact assessment (PIA) of the Census to be held in 2026. This PIA forms the second phase of a three phase PIA process and focuses on the Census design and build – with particular attention to activities and practices that will be different in 2026 compared to previous Census cycles. Therefore, this PIA identifies aspects of the Census that are changing and assesses those changes (including new approaches to personal information handling) against the requirements of the *Privacy Act 1988* (Cth).

IIS would like to thank the many people at the ABS who assisted IIS during the development of this PIA, along with those stakeholders who provided invaluable feedback on proposals and draft recommendations.

1.1 IIS's overall view

Overall, IIS finds that the ABS is taking appropriate steps to meet its obligations under the Privacy Act in relation to the Census design and build. The ABS's privacy governance arrangements are mature and appear to be functioning effectively – this was particularly evident when reviewing activities that had already been the subject of an internal Privacy Threshold Assessment (PTA).

During the analysis conducted for this PIA, IIS reviewed a range of matters including:

- Temporary Workforce recruitment and management and use of the Safe Zone app by field officers
- Special Dwelling Enumeration
- Use of the front-of-form address
- ABS engagement via social media and collection of user information in limited circumstances
- Use of myGov as a pathway to the online Census form
- Development and use of the Whole of Australian Government (WoAG) Coding Capability to code Census data
- Development and use of a Synthetic Test Dataset
- Collection and use of administrative data¹ to assist with determining Census night dwelling occupancy
- Use of administrative data to impute high-level information for non-responding households
- Use of Census data to enhance the Business Locations Asset (BLA).

IIS assessed each of these matters against relevant Australian Privacy Principles (APPs) to check compliance with the Privacy Act. On the whole, we found that the ABS had controls in place to manage privacy risks and ensure compliance.

¹ Administrative data is information collected by government agencies, businesses or other organisations for various purposes, including registrations, transactions and record keeping, usually during the delivery of a service.

The most substantive recommendations made in this PIA relate to use of administrative data in the Census and aim to ensure use limitation and a structured, repeatable approach to addressing data ethics questions. Those recommendations join earlier recommendations made in the Phase 1 PIA regarding administrative data use.

A major theme of other recommendations is ensuring open communication and clarity about ABS data handling – particularly with regard to new projects or activities involving Census data or associated personal information. The purpose of those recommendations is to reduce the risk of public misunderstanding and encourage ongoing social acceptance.

1.2 Summary of recommendations

In this PIA, IIS makes 10 recommendations. A high-level summary of recommendations appears below, with the full recommendations appearing in the body of the report.

Recommendation 1 Compliance	Train relevant staff members in appropriate handling of candidate personal information and use of the recruitment system.
Recommendation 2 Compliance	Ensure myGov privacy information makes clear possible additional uses of myGov by the ABS beyond the Census.
Recommendation 3 Best practice	Publish explanatory information about Census coding on the ABS website.
Recommendation 4 Compliance	Include information about administrative data collection and use in the Census 2026 Privacy Statement.
Recommendation 5 Best practice	Test the effectiveness of awareness raising activities in relation to administrative data use in the Census.
Recommendation 6 Best practice	Restrict use of non-PLIDA administrative data collected for determining Census night occupancy
Recommendation 7 Best practice	Remove administrative data used for determining Census night occupancy from Census systems five years after Census 2026.
Recommendation 8 Best practice	Take a structured approach to data ethics oversight of proposed administrative data uses in the 2026 Census.
Recommendation 9 Best practice	Clarify the ABS's use and retention of address information (including use for BLA related processing) in the 2026 Census Privacy Statement.

Recommendation 10	Test that BLA-related privacy arrangements are fit for purpose during 2025
Best practice	Operational Readiness Exercise (ORE).

2. Introduction

2.1 Background

The ABS conducts the Australian Census of Population and Housing (the Census) every five years. It seeks to count every person and household in Australia to provide a comprehensive snapshot of the country on a single night (i.e. Census night). The Census form asks questions about every person in the household including, among other things, their age, country of birth, religion, ancestry, language used at home, work and education. The next Census will occur in 2026.

Census data can be used in a variety of ways by a diverse range of researchers. The 2021 Census data was published in a three-phased approach accessible through various Census data tools.² Census data is also integrated with other datasets to form the Person Level Integrated Data Asset (PLIDA) (previously Multi-Agency Data Integration Project (MADIP)). The PLIDA provides whole-of-life insights about population groups in Australia, such as the interactions between their characteristics, use of services like healthcare and education, and outcomes like improved health and employment.

The 2026 Census is being run in an environment where privacy is increasingly important to the public and where government agencies risk significant backlash if the information they hold is misused, breached or used in ways that are outside individual expectations. In acknowledgment of this, the ABS has prepared a 2026 Census PIA Plan, which commits to managing, minimising, or eliminating potential privacy impacts of the 2026 Census through a Privacy by Design approach and the commissioning of comprehensive and independent PIAs. The ABS is undertaking a phased approach to the PIAs for the 2026 Census:

- **Phase 1 PIA** – Preparation, planning and development (March to September 2023)
- **Phase 2 PIA** – Build and design (March to September 2024) (*this PIA*)
- **Phase 3 PIA** – Testing operational readiness (March to June 2025).

IIS undertook Phase 1 of the 2026 Census PIA in 2023. IIS was engaged again by the ABS to undertake Phase 2 of the 2026 Census PIA, which is the subject of this report.

2.2 Scope of this assessment

The scoping of the Phase 2 PIA was a dynamic and iterative process.

First, the 2026 Census Plan provided an array of potential topics to be considered in the Phase 2 PIA. IIS then met with teams (both inside and outside the Census division) along with the Census privacy team. From these interviews (and supporting documentation), IIS independently formed an initial position on the privacy issues and risks arising from the build and design stage of the 2026 Census. This position was shared with the ABS. IIS then compared its position to the privacy issues and risks that the ABS had identified internally.

² See ABS, [Census 2021 product release guide](#).

Following this process, the following areas were identified as requiring assessment in this PIA:

- Temporary Workforce recruitment and management
- Special Dwelling Enumeration
- Use of the front-of-form address
- ABS engagement via social media and collection of user information in limited circumstances
- Use of myGov as a pathway to the online Census form
- Development and use of the WoAG Coding Capability to code Census data
- Collection and use of administrative data to assist with determining Census night dwelling occupancy
- Use of administrative data to impute high-level information for non-responding households
- Use of Census data to enhance the BLA.

IIS also reviewed use of the SafeZone app by field officers and development of a synthetic test dataset to allow safe testing of Census-related data processing. Both of these matters had already been the subject of internal PTAs. IIS reviewed the PTAs and was satisfied with the process the ABS followed to assess and address possible privacy risks.

For each of the matters listed above, IIS gained an understanding of key personal information involved and proposed data flows along with controls already in place to manage privacy risks. We then assessed each item against relevant APPs to identify possible risks of non-compliance and opportunities for privacy enhancing improvements. The PIA makes recommendations to address possible gaps in compliance or privacy risk areas. It also gives regard to steps the ABS can take to foster public trust and social acceptance in relation to new activities occurring during the 2026 Census cycle.

2.3 Relevant legislation

Privacy Act

The ABS is covered by the *Privacy Act 1988* (Cth) and its 13 Australian Privacy Principles (APPs). The APPs set rules for the handling of personal information which the Act defines as any 'information or any opinion about an identified individual or an individual who is reasonably identifiable' (s 6(1)). The APPs impose a range of privacy obligations on entities. The APPs also give individuals certain rights and choices in relation to their personal information which individuals can pursue under the Privacy Act's complaint-handling and enforcement provisions.

As an agency, the ABS is also covered by the [Australian Government Agencies Privacy Code](#) which sets out specific requirements and key practical steps that agencies must take as part of complying with APP 1.2. It requires agencies to move towards a best practice approach to privacy governance to help build a consistent, high standard of personal information management.

The ABS's legislation

The ABS is authorised to collect, compile, analyse, and publish statistics under the *Australian Bureau of Statistics Act 1975* (Cth) (ABS Act) and the *Census and Statistics Act 1905* (Cth) (Census and Statistics Act).

The ABS Act establishes the ABS as an independent statutory authority, defines the functions of the ABS, establishes the office of Australian Statistician and describes the terms under which the Australian Statistician can be appointed to, and removed from, office. The Census and Statistics Act gives the Australian Statistician the authority to conduct the Census. While the ABS publishes statistical outputs, these must not be published or disseminated in a manner that is likely to enable the identification of a particular person or organisation (s 12(2)).

Practically speaking, this means that the ABS only publishes or disseminates confidentialised and aggregate statistical products. The ABS also supports controlled researcher access to de-identified unit-level Census data in its own secure environment (DataLab), subject to the Five Safes Framework.³

2.4 Census privacy governance

APP 1.2 promotes a privacy by design approach by requiring entities to take reasonable steps to implement practices, procedures and systems to ensure compliance with the APPs and any binding registered APP code. Relevantly for the ABS, it must comply with the Australian Government Agencies Privacy Code, which requires agencies to take a series of steps to embed privacy into their practices.⁴

The ABS has robust internal privacy governance arrangements, including a regularly monitored Privacy Management Plan, dedicated roles and committees with privacy responsibilities, privacy assessment processes, and a range of internal policies and procedures to help meet its obligations under the Privacy Act and the Australian Government Agencies Privacy Code.

For the Census in particular, the ABS has developed a 'Privacy Strategy 2021-28' to ensure that privacy is considered across multiple Censuses, inclusive of the 2026 Census. The strategy sets out goals and focus areas of action to encourage ongoing improvement to management of personal information and to maintain community trust. The ABS also has a 2026 Census Data Protection Plan that sets out the principles, obligations, roles and responsibilities, and rules for the handling and protection of Census data.

Privacy for the 2026 Census is supported by the following roles:

- *Census Privacy Team* – Provides ongoing privacy support and awareness raising within the 2026 Census Program; coordinates the Census Privacy work program; facilitates the PIA processes, including implementation of recommendations from PIAs and other review and assurance

³ See ABS, 'Five Safes Framework'.

⁴ See OAIC, 'Privacy (Australian Government Agencies – Governance) APP Code 2017'.

processes; works closely with the ABS Privacy Officer and Privacy Section to ensure consistency of messaging, advice and practice.

- *Census Privacy and Data Protection Working Group* – Provides advice on privacy matters, taking into account the importance of community participation and high-quality data for the Census. The Group is chaired by the General Manager Census and membership includes senior Census staff, the ABS Privacy Officer, ABS internal stakeholders and external representatives.
- *Census Data Protection Officer* – Role within the Census Privacy Team that helps to implement the Census Data Protection Plan, working in collaboration with Census data stewards and statistical managers.
- *Census Independent Privacy Advisor (CIPA)* – The CIPA has been engaged throughout the 2026 Census cycle to enhance privacy practices, identification of emerging risks and provides advice on privacy legislation. CIPA is a member of Census Privacy and Data Protection Working Group and regular meetings are held between Census Senior Executive to provide specialist privacy advice and discuss key privacy matters.

2.5 Approach to this PIA

The following sections outline IIS's approach to developing the PIA and analysing privacy issues.

Discovery and issues guidance

IIS undertook an initial review of ABS documents to consider developments since the Phase 1 Census 2026 PIA and the array of potential Phase 2 PIA in-scope topics under consideration. These included:

- Previous Census privacy material
- 2026 Census planning documents, and
- Personal information mapping questionnaires completed by relevant business units.

IIS then interviewed key ABS staff members to discuss in-scope elements, clarify our understanding and receive input. The initial list of internal stakeholders was based on the business units which completed the Personal Information Mapping questionnaires for the Phase 2 PIA. A full list of documents reviewed, and ABS meetings held, is at [Appendix B](#).

Following this early discovery process, IIS prepared an 'initial scoping' document which was cross-checked against the ABS's internal list of privacy issues and risks. From this process, IIS developed an internal 'issues guidance' document for the ABS, which was used to establish common ground for the rest of the PIA process. For each in-scope element, the document set out the following:

- Overview of the situation, including the ABS's plans or proposals
- Possible privacy implications
- Areas that would benefit from additional information or clarification from the ABS
- Where applicable, consultation questions that could be put to external stakeholders.

IIS held follow-up meetings with the ABS to address further information gathering needs and clarify PIA scope. The issues guidance document provided the basis for the consultation paper that IIS prepared for stakeholder engagement.

Stakeholder engagement

Open engagement is an important part of the Census design process. Consistent with the approach of the Phase 1 PIA, the ABS intended for the Phase 2 PIA to involve consultation with external stakeholders.

IIS and the ABS agreed to hold consultations in the form of roundtables with key stakeholders. The stakeholder list was put together by IIS with ABS input, and included privacy and advocacy groups, civil society groups, regulators, academics, and data and ethics experts.

The stakeholders were selected based on their:

- Representation of key sectors of Australian society
- Special interest or expertise
- Prior contribution to ABS PIA consultations.

See [Appendix C](#) for a full list of stakeholders.

The objectives of the consultation process were to:

- Inform stakeholders about certain activities and opportunities that the ABS is considering for the 2026 Census
- Seek stakeholder input on those activities and opportunities.

IIS prepared and distributed to stakeholders a Consultation Paper that provided background on the key topics in scope, along with associated guiding questions. In June 2024 IIS held one virtual roundtable session with a group of stakeholders and two virtual meetings with individual stakeholders who were not able to attend the roundtable. Stakeholders were able to offer feedback during the session and afterwards. They were also given the opportunity to provide a written submission.

IIS then prepared an internal consultation report for the ABS, which summarised stakeholder feedback on the key elements that were discussed. The stakeholders provided valuable contributions which IIS has incorporated into our privacy analysis, subject to some limitations which we discuss below.

Preliminary findings and recommendations

Following the methodology of the Phase 1 2026 Census PIA and as agreed with the ABS, IIS prepared preliminary analysis and recommendations to 'bench test' with the external stakeholders. This involved IIS analysing the privacy issues taking into account feedback from stakeholder consultations. The draft PIA recommendations were shared with the ABS and the same external stakeholders.

The bench testing was intended to provide external stakeholders with a second opportunity to present their views and clarify any matters arising from the draft PIA recommendations. IIS took account of stakeholder feedback in the drafting of this PIA report.

2.6 About this report

The Phase 1 PIA took a high-level, big picture approach to the privacy analysis, applying core privacy principles to identify risks and opportunities for best practice. This PIA engages more closely with the specific requirements of the APPs and the Privacy Act.

The report is organised according to topic with each section offering a description of what is changing in relation to the topic followed by an analysis of data flows against key APPs. Each section concludes with a summary of the findings and, if applicable, a recommendation to address any identified gaps in compliance or privacy protection. Recommendations also identify opportunities for implementing best practice arrangements that go beyond baseline compliance.

- *Executive summary* (Section 1) – including a summary of recommendations.
- *Introduction* (Section 2) – provides background on the PIA, its scope, the wider PIA context including the phased PIA approach, the legislative framework and a snapshot of personal information flows.
- *Privacy analysis of key issues* (Section 3 to Section 10) – analyses key issues against the APPs and makes recommendations to mitigate risk and improve practice.
- *Glossary* (Appendix A).
- *Documents reviewed and meetings held* (Appendix B) – lists documents reviewed and meetings held as part of the information gathering process.
- *List of stakeholders* (Appendix C) – lists stakeholders who participated in roundtable consultations and/or who provided written submissions as part of the Phase 1 PIA process.
- *Overview of key personal information flows* (Appendix D) – contains a diagram of the key data flows involved in the Census.

For each issue analysed in Sections 3 to 10, IIS has offered some contextual information about the main team with oversight of the issue – however not all issues affect only one team, and not all teams are covered. The analysis has been issues focused.

2.7 Personal information flows

The Census is a major logistical undertaking and as such involves a range of personal information flows. A diagram offering an overview of key personal information flows is provided in Appendix D. Those personal information flows include:

- *Temporary workforce* – Collection and handling of candidate and temporary workforce employee information to enable workforce management.

- *Customer service* – Collection and handling of information about individuals interacting with the call centre or online self-service tools.
- *Social media* – Collection and handling of information about social media users in limited circumstances.
- *Statistics* – Collection and processing of paper and online Census forms and related forms (e.g. Special Dwelling Enumeration).
- *Administrative data* – Collection and handling of information collected from third party data custodians to support Census-night occupancy determinations and imputation for non-responding households.
- *Processing and coding* – Processing of statistics information (including validation of address information) and coding of data.
- *Use of statistics in other data assets* – Processing of Census data (including data integration) to enable use of Census data in other data assets (e.g. PLIDA, the BLA, the Address register).
- *Dissemination* – Preparation of de-identified datasets for dissemination (e.g. via DataLab).

This PIA focuses on those data flows that are new or changing in 2026. In the body of the report, each issue is described then key stages in the information lifecycle are analysed against the requirements of the APPs.

3. Enumeration including special dwelling enumeration

The Enumeration team looks after all aspects of the Census enumeration model – that is, all the different ways in which the ABS provides the Australian public with Census materials and supports them completing the Census. The team plays both a planning and operational role. During the Census, the Enumeration team deploys field staff to count dwellings and remind households to complete the Census. While most Australians will complete the Census either online or via a paper form, Australians living in remote areas or special dwellings may require additional support.

3.1 Changes expected in 2026

Generally, the Enumeration team is using the same model as in 2021 with some minor changes including:

- *Introduction of operational support centres in certain regional areas* – standing up a local office and teams to support enumeration activities (e.g., western NSW).
- *Use of administrative data to improve dwelling occupancy verification* – to enable more targeted follow up with non-responding households (see [Section 9](#) below).

During the scoping process for this PIA, the ABS also suggested IIS give attention to:

- *Special dwelling enumeration* – the ABS has arrangements in place to enable enumeration of special dwellings (e.g. hotels, hospitals, aged care facilities, prisons, mining camps, etc.) and vulnerable populations (e.g. people staying at women’s shelters, people experiencing homelessness). IIS understands a minor change for 2026 will be that the ABS will use a platform called Informatica to receive information regarding special dwellings.

3.2 Personal and other information involved

Personal information handled by the Enumeration team includes:

- Statistical information (Census) – collected via physical Census forms (and other types of forms) and handled by field staff as part of the enumeration process.
- Personal information (about members of the public) – collected during administrative activities (e.g., contact details for service providers).
- Personal and sensitive information (about temporary workforce) – collected to enable recruitment of temporary workforce to assist with Census operations (see [Section 4](#) below).

Regional operations support centres

IIS did not identify any specific privacy risks in relation to a high-level review of plans for the standing up of regional operations support centres. One possible issue discussed with the ABS was field staff operating in remote areas with limited internet coverage and how this may result in weaker information management practices (for example, storing documents temporarily either on local devices or in hard

copy until internet was available or emailing documents rather than uploading direct to secure ABS systems). The ABS informed IIS that it was exploring the use of Starlink to provide internet coverage in remote areas. We also note Recommendation 1 below, which refers to training field managers in appropriate handling of candidate personal information.

Special dwelling enumeration

Special dwelling enumeration is concerned with managing the enumeration of non-private dwellings such as hotels, hospitals, aged care facilities, prisons, mining camps and so on. In order to ensure that people staying in these locations are counted in the Census, the ABS works with a key contact in the special dwelling (for example, a hotel clerk or a hospital administrator). The key contact may help with distributing Census forms or reminding those in the establishment to participate in the Census on Census night.

In some cases, where it is impracticable to have people at the special dwelling fill out a Census form, the key contact may submit high-level information about each person staying at the special dwelling. IIS understands that this high-level information includes about twelve variables including age, sex and usual address (if applicable). This approach to enumerating special dwellings has not changed significantly since the last Census. The main change is that, in previous Censuses, the key contact filled out a spreadsheet with high-level information and emailed it to the ABS. In 2026, key contacts will fill out a template document and upload it to an ABS-designed platform called Informatica.

3.3 APP analysis and other privacy risks

Note that use of administrative data is covered in [Section 9](#) and collection and handling of temporary workforce information is covered in [Section 4](#). The ABS’s approach to Special Dwelling Enumeration has not changed significantly from years past, therefore our APP analysis focuses on those elements that are new in 2026 or warrant closer attention – specifically, we focus on the key contact’s collection and upload of personal information to ABS systems. In our view APPs 3 (Collection), 5 (Notice) and 11 (Security) are relevant here.

APP	Comments and analysis
APP 3	<p><i>Collection of personal information about individuals staying in ‘Special Dwellings’</i></p> <p>IIS understands that the key contact would gather high-level information about the individuals staying in the special dwelling on Census night and enter it in a template document provided by the ABS. (This information would cover all individuals who do not, or are not able to, fill out a Census form for themselves.) The key contact would then upload the completed template document to the ABS’s Informatica platform.</p> <p>APP 3 requires an agency to only collect personal information that is reasonably necessary for or directly related to one or more of the agency’s functions or activities. We find that this collection of information in connection with the Census meets this requirement.</p> <p>No further issues identified.</p>

APP	Comments and analysis
	<p><i>Collection of sensitive information about individuals staying in ‘Special Dwellings’</i></p> <p>It was unclear to IIS whether any of the information to be collected and submitted to the ABS by the key contact in a special dwelling might meet the definition of sensitive information which accrues some higher protections under the APPs. Specifically, APP 3.3 requires an agency to obtain consent prior to collection of sensitive information unless an exception applies.</p> <p>IIS finds that the ABS’s collection of sensitive information during this process is likely to be permitted by the exception under APP 3.4(a) allowing collection of sensitive information where the collection is required or authorised by or under an Australian law. APP 5 notification requirements will still apply (see below) and the key contact should make best efforts to notify the individual or a person acting on behalf of the individual (for example a spouse or relative) where the individual themselves lacks capacity to read or understand information contained in the notification (this may be particularly relevant to special dwellings that are hospitals or aged care homes).</p> <p>We also find that the collection meets the fair and lawful requirement under APP 3.5, though fairness will be strengthened by good transparency and notification practices – see APP 5.</p> <p>No further issues identified.</p>
APP 3.6	<p><i>Indirect collection of personal information</i></p> <p>APP 3.6 states that an agency must only collect personal information directly from the individual unless either: the individual consents to the indirect collection, or, the agency is required or authorised by or under law to collect the information indirectly, or, it is unreasonable or impracticable to collect the information directly.</p> <p>Where a key contact at a special dwelling submits high-level information about residents or guests to the ABS, this would generally be considered an indirect collection. It was not clear to IIS whether key contacts attempt to seek consent from individuals where possible, (and where the individual has the capacity to consent). In our view, indirect collection of this information by the ABS is likely to be permitted by the exception allowing indirect collection where authorised by law. We also note that the ABS has a preference towards direct collection and, where possible, prefers an individual staying at a special dwelling on Census night to fill in a form.</p> <p>No further issues identified.</p>
APP 5	<p><i>Notifying people staying in a special dwelling of personal information collection</i></p> <p>APP 5 requires an agency to take reasonable steps to make an individual aware of certain matters when collecting information about them (usually this takes the form of a collection notice). IIS assumes that, as this type of data collection involving special dwellings has</p>

APP	Comments and analysis
	<p>occurred in past Censuses, the ABS has arrangements in place (with the help of the key contact) to make individuals aware of the information they are collecting. Having an effective notification mechanism in place for special dwellings is particularly important given that collection is indirect.</p> <p>No further issues identified.</p>
APP 11	<p><i>Security of personal information</i></p> <p>IIS has not closely reviewed the operation of Informatica during this PIA but understands that the platform aims to improve the security of the data collection process by removing less reliable forms of transmission such as transfer via email. We understand that once the information is collected via the Informatica platform it is processed to allow imputation into Census datasets at which point it is subject to the same security and retention arrangements as other Census data. One minor consideration may be to ensure that special dwelling key contacts dispose of any filled out templates (containing personal information) stored on their local devices after upload to the ABS's systems. If it does not do so already, the ABS should advise key contacts to do this during any offboarding process.</p> <p>No further issues identified.</p>

3.4 Summary

The changes to special dwelling enumeration appear to be minimal and use of the Informatica platform would appear to further reduce privacy and security risks by reducing the emailing of personal information. IIS identified possible minor improvements to privacy arrangements (outlined in the analysis above) but no gaps in privacy compliance.

4. Temporary workforce

The Temporary Workforce team is responsible for the end-to-end cycle of recruitment, training, Work Health and Safety, onboarding, employee management, offboarding, payroll and support services for temporary field, office and warehouse staff working on the Census. The field staff are managed and directed by the Enumeration team. To conduct its functions and activities, the team will collect and handle a range of personal information about applicants and employees. The team anticipates that it will receive over 130,000 applications and onboard 35,000 employees for the 2026 Census.

The team is in the process of procuring external vendors for (i) managed payroll services, (ii) a recruitment solution, and (iii) personal safety devices. IIS understands that the Temporary Workforce will have systems and processes ready for the 2025 ORE.

4.1 Changes expected in 2026

Overall, the Temporary Workforce team will be reusing the same business model as 2021, however recruitment processes will be delivered in-house in 2026. This is a change from 2021, where recruitment was undertaken through an external provider. The Temporary Workforce team is anticipating the following changes for the 2026 Census:

- *Changes in payroll* – to improve efficiency, increase frequency of payment.
- *Internal management of the recruitment system* – the recruitment system will be externally provided (likely a cloud-based solution) but internally managed.
- *Field-based hiring managers recruiting field staff* – certain field managers will be able to recruit field staff meaning managers will have access to the recruitment system that they previously did not have.
- *Coding of candidate addresses to align with Address Register* – exploring the ability for candidates' addresses to be coded in the recruitment system according to Census geographical boundaries held in the Address Register, to assist with planning purposes.

IIS understands that the SafeZone app will be used for check-in/check-out and to support field staff safety (this is an existing solution used in the 2021 Census and by other ABS interviewers and has been subject to a PTA).

4.2 Personal and other information involved

Personal information handled by the Temporary Workforce team includes:

- Personal and sensitive information (Temporary Workforce) – broad range of personal information collected and used as part of initial application and onboarding, as well as ongoing employee management and support.

4.3 APP analysis and other privacy risks

IIS has given particular attention in our APP analysis to those processes that will be different or new in 2026. With regard to those items, we find that APPs 1 (Governance), 6 (Use and Disclosure) and 11 (Security) are most relevant.

APP	Comments and analysis
APP 1	<p><i>Training of staff managing and accessing the recruitment system</i></p> <p>With the move to internal management of the recruitment system (via an external platform), the ABS should ensure appropriate training for staff managing and accessing recruitment systems to minimise risks of information misuse. This goes to compliance with APP 1.2(a).</p> <p>See Recommendation 1.</p> <hr/> <p><i>Training of field-based hiring managers in collection and handling of candidate personal information</i></p> <p>The ABS has advised that most candidate personal information will be collected in digital form, but that in some exceptional circumstances hardcopy information may be collected. Where field-based hiring managers act as a conduit for candidate personal information during recruitment, the ABS should ensure managers receive training on appropriate collection and handling of the information, including hardcopy information and sensitive information. This goes to compliance with APP 1.2(a). IIS also understands that the ABS is exploring use of Starlink to enable internet coverage in remote areas to reduce the need for collection of personal information in hard copy form or saving of information on local devices.</p> <p>See Recommendation 1.</p>
APP 6	<p><i>Coding of candidate addresses to align with the Address Register</i></p> <p>This constitutes a new use of candidate personal information. The purpose of this use is to support planning and resource allocation. IIS finds that this use complies with APP 6.2(a). In the interests of transparency and to meet the APP 6.2(a) reasonable expectations test, the ABS could consider giving a brief explanation of its use of address information in its APP 5 privacy notice to candidates and employees. That said, use of address information for planning and resource allocation is likely to be expected and anticipated by candidates and employees.</p> <p>No further issues identified.</p>
APP 11	<p><i>Procurement of new vendors for recruitment and payroll</i></p> <p>The ABS advised that it is pursuing a new IT solution (for recruitment) and a new IT solution and service (for payroll), both provided by an external vendor. While overarching recruitment and payroll approaches remain the same, the solutions used will be different</p>

APP	Comments and analysis
	<p>in 2026. The ABS advised IIS that its procurement and contract management arrangements include a strong focus on privacy requirements in statement-of-requirements documentation.⁵ Additionally, in response to recommendation 11 of the 2021 PIA, the ABS has created a register to monitor privacy requirements in contracts.⁶</p> <p>No further issues identified.</p> <hr/> <p><i>Security of the recruitment system</i></p> <p>With the move to internal management of the recruitment system (via an external IT solution), IIS understands that the ABS will apply its standard information security arrangements, in line with its Census Security Strategy, Cyber Security Policy, and Protective Security Framework. According to the ABS, access controls will apply, managed through the Temporary Workforce team. Further review of security arrangements of the recruitment system may be a matter for the Phase 3 PIA.</p> <p>No further issues identified.</p> <hr/> <p><i>Retention of personal information in recruitment and payroll systems</i></p> <p>The ABS has advised that candidate and staff personal information will be disposed of after 7 or 75 years, depending on employment arrangements and in accordance with the relevant Records Authority. Disposal requirements will be included in vendor contracts.</p> <p>No further issues identified.</p> <hr/> <p><i>Field-based hiring manager access to the recruitment system</i></p> <p>The ABS has advised that, in line with the principle of least privilege, field-based hiring managers will only have access to candidate records within their geographic zones of operation. Such access arrangements should be tested in the 2025 ORE.</p> <p>See Recommendation 1.</p>
Other risks	Comments and analysis
N/A	<p><i>Field officer use of the SafeZone app</i></p> <p>Field officers will be required to use the SafeZone app which shares location information with the ABS for Work Health and Safety purposes. The app was used in the 2021 Census and has been subject to a PTA and two security assessments. IIS reviewed the</p>

⁵ See Census Privacy Strategy 2021-28, p 5.

⁶ See Census Privacy Strategy 2021-28, p 5.

APP	Comments and analysis
	<p>PTA, including the privacy notice that will be made available to field staff via the WDB WHS Hub, and was satisfied with the assessment and privacy controls in place.</p> <p>No further issues identified.</p>

4.4 Summary and recommendations

Only minor changes appear to be planned for activities involving the temporary workforce, therefore our analysis has been fairly narrow in assessing possible privacy risks. A key consideration is ensuring appropriate handling of personal information in the field, particularly in circumstances where field managers may have greater access to candidate information.

Recommendation 1 – Train relevant staff members in appropriate handling of candidate personal information and use of the recruitment system

Compliance recommendation

Ensure staff (including field-based hiring managers) receive training in appropriate handling of candidate personal information including any hard copy information submitted by candidates during the recruitment process. Training should also include appropriate use of the recruitment system.

Arrangements involving the recruitment system (including field-based hiring manager access control) should be tested during the 2025 ORE, if practicable.

5. Customer experience and engagement via social media

The Customer Experience team is responsible for developing the suite of content, channels and touchpoints for the Census. Specifically, this involves building a new website, research and development to inform a national advertising campaign, customer service channels (including delivery of the contact centre and Census website) and developing material both for staff and for the public to help them participate (Census letters and envelopes). As with the 2021 Census, the ABS will use Services Australia as the contact centre provider for the 2025 ORE and 2026 Census. At operational time, the team also manages media and social media engagements (proactively and reactively).

The team will be working through the data flows for how personal information will flow from the self-service Contact Us channel through to downstream systems before the Census website goes live in July 2025. This is likely to involve the same process used in the 2021 cycle, which involved using the Census Agent Tool (CAT) and an access restricted HCL Notes database.

Along with developing the key public-ABS touchpoints for the Census, the Customer Experience team also conducts research and has initiated the first round of audience segmentation research that will explore public attitudes towards the Census, including the collection of sensitive information, perceptions of data sharing, and sharing of historical or current datasets with other agencies. The team is aware of the Phase 1 PIA recommendation with respect to regular testing of community perceptions and is actively factoring this into their research.

5.1 Changes expected in 2026

The Customer Experience team anticipates that most of its arrangements will be very similar to those in place for the 2021 Census. The team advised that it is still working through whether the ABS will use the same process and system for Refusals or move to a new system in 2026; technical details are not yet available. Therefore, this matter will be taken up in the Phase 3 PIA.

While not a new issue or process, the team carries out the following activity that has not been assessed in previous Census PIAs:

- *Personal information collected via social media* – the ABS receives messages from the public across all its social media platforms and uses Nuvi, a social media management platform, to process and respond to messages. At times the ABS collects the handle and messages of individuals that engage in repeat misbehaviour or indicate a risk of self-harm. While this is not a new collection or use of personal information for the 2026 Census, it has not been considered in previous PIAs and therefore has been addressed in the APP analysis below.

The Customer Experience team advised IIS that it was procuring an AI chatbot for the Census website (but not the Census Digital Service, the Census landing ('Page 1') or ABS website) to assist people in finding information on the website. The chatbot will potentially use Large Language Models, a type of AI program built on machine learning. The chatbot would not be available within the online Census form.

Rather, it would be limited to serving existing information from the Census website only. The ABS advised IIS that the chatbot solution will not capture personal information. It further advised IIS that the RFQ for the chatbot specifically requires no capture of personal information. Given the chatbot will not collect personal information, the APPs are unlikely to apply, therefore the chatbot has not been considered in the analysis below. IIS does note, however, **Recommendation 3** and the importance of transparency in relation to use of AI and LLMs.

5.2 Personal and other information involved

Personal information handled by the Customer Experience team includes:

- Personal information (members of the public) – collected via the contact centre (phone) and self-service (online) channels; typically, this includes name, contact details, address and the presenting issue/query.
- Personal information (members of the public) – collected via social media platforms in the course of engaging with and responding to members of the public on social media.

The Customer Experience team also handles personal information in relation to community engagement (e.g. contact details of MPs or community groups) and research (e.g. information about participants in surveys or focus groups). This information is out of scope for the Phase 2 PIA.

Engagement via social media

The ABS advised that during the Census, social media acts as a key customer service channel. The ABS disseminates paid advertising on social media that is geo-targeted. The social media team respond to public comments on paid Census campaign advertising. People can send direct messages to the ABS via a social media platform (e.g. Facebook, Instagram, LinkedIn, X) and those messages may include personal information such as name/handle, address, phone number, query, information about physical or mental health, capacity to complete the Census and so on.

To manage social media engagement, the ABS uses Nuvi (a social media management platform) to allow the ABS to triage and respond to messages systematically. The ABS advised that Nuvi does not download social media content – only filters and gives visibility to messages and posts addressed to the ABS within the various platforms, allowing, for example, grouping together of similar questions and themes to facilitate a quick and consistent response. The ABS advised that it does not store personal information from social media in its systems, except in cases where it needs to record: (i) people engaged in repeated misbehaviours, and (ii) the details of someone whose message indicates risk of harm.

5.3 APP analysis and other privacy risks

IIS has briefly reviewed the ABS's practices below – noting that the ABS also uses social media outside of the Census and has policies in place that govern its social media use. With regard to ABS use of social media, we find that APPs 1 (Governance), 3 (Collection), 5 (Notice), 6 (Use and Disclosure) and 11 (Security and disposal) are most relevant.

APP	Comments and analysis
Definition of PI	<p><i>Social media user information and the definition of personal information</i></p> <p>As outlined above, at times the ABS may collect and store information about individuals that communicate with the ABS via social media. That information may include the name or handle of the individual along with messages the individual has sent to the ABS. Social media handles will not always reveal the identity of the individual but may do so in some cases. Other information associated with the user (for example, information included in a social media post or message to the ABS) may also include personal information. For these reasons, IIS suggests the ABS treat all such information as personal information and apply the appropriate privacy protections.</p>
APP 1	<p><i>Governance arrangements applying to the ABS's social media use</i></p> <p>The ABS advised IIS that internal policies and procedures govern its use of social media, including its response to repeat misbehaviour and individuals indicating risk of self-harm. According to the ABS, those policies and procedures govern the ABS's agency-wide use of social media, not only that occurring during the Census. IIS did not review social media policies and procedures as this fell outside the scope of the Phase 2 PIA.</p> <p>No further issues identified.</p>
APP 3	<p><i>Collection of personal information about users of social media</i></p> <p>The ABS stated that most of its engagement with individuals via social media occurred on the relevant platform with the ABS generally not collecting and storing social media user information in its own systems. IIS understands that there are two exceptions to this rule: 1) where a social media user engages in repeat misbehaviour (such as abusive language), and 2) where a social media user's message content indicates a possible risk of self-harm. In such cases, the ABS may collect the person's name/handle along with a screenshot of the post/message and the ABS's response. The purpose of this collection is to allow the ABS to manage the incident appropriately, record its response and ensure appropriate support to staff members as part of its duty of care to employees.</p> <p>APP 3 states that an agency must not collect personal information unless the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities. We find that the ABS's collection of the information outlined above is reasonably necessary to incident management (associated with customer service) and managing its duty of care to employees.</p> <p>No further issues identified.</p> <hr/> <p><i>Collection of sensitive information about users of social media</i></p> <p>In some limited cases, the ABS may, in the course of collecting information in the manner outlined in the row above, collect information about the mental health of a social media user (for example, where the user sends a message via social media indicating a risk of</p>

APP	Comments and analysis
	<p>self-harm). Generally, an agency may only collect sensitive information with the consent of the individual, unless another exception under APP 3.4 applies. It is arguable that if an individual proactively sends a message to an agency via social media, they impliedly consent to that agency collecting that message and associated information. However, in the case of an individual experiencing a mental health crisis, for example, the individual's capacity to consent may be impaired.</p> <p>In such cases, IIS believes collection of the information may be permitted by APP 3.4(b) and the exception set out in s 16A (Permitted General Situations) allowing collection of sensitive information where the agency reasonably believes that the collection is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety, <i>and</i> it is unreasonable or impracticable to seek consent. This provision requires that the threat to life, health or safety is serious – the threat does <i>not</i> have to be imminent. The ABS advised that it would generally only collect this information to enable reporting if there is a serious risk and record keeping in case it's a repeated contact. This appears to fall within the scope of APP 3.4(b).</p> <p>No further issues identified.</p>
APP 5	<p><i>Notice of collection of personal information via social media</i></p> <p>When collecting personal information, APP 5 requires an agency to take such steps (if any) as are reasonable in the circumstances to make the individual aware of certain matters about the collection. The ABS will be collecting personal information from social media only in very limited circumstances. IIS finds that the nature of those circumstances, outlined above, means that it is reasonable to take no additional steps to provide a privacy notice. In coming to this view, IIS has taken into account that individuals interacting with the ABS via social media will be aware of the identity of the ABS and its general role in relation to statistics and the Census from the sorts of messages the ABS posts to social media. In knowing the identity of the ABS, an individual is equipped to find the ABS's website, seek out privacy information or contact the ABS on their own initiative. The previous Census 2021 Privacy Statement contained some general information about personal information collected for non-statistical purposes. Further engagement with individuals involved in repeat misbehaviour or experiencing mental health challenges in relation to privacy is unlikely to be reasonable or productive.</p> <p>No further issues identified.</p>
APP 6	<p><i>Use of information collected via social media</i></p> <p>APP 6 requires an agency to only use personal information for the primary purpose it was collected unless an exception applies. IIS understands that the ABS collects the information in question for the purposes of incident management (associated with customer service) and managing its duty of care to employees. These uses fall within the primary purpose of collection. We are not aware of any secondary uses.</p>

<i>APP</i>	<i>Comments and analysis</i>
	No further issues identified.
APP 11	<p data-bbox="336 439 655 472"><i>Security and data disposal</i></p> <p data-bbox="336 495 1409 763">At the time of writing, IIS was not aware of the arrangements in place to store information collected from social media, nor the systems used. Given the possible sensitivity of the information (for example, where it contains information about an individual's mental health), IIS would expect the ABS to apply strong security arrangements to the information and strict access controls. Regarding disposal, the ABS advised IIS that such records would be destroyed five years after the 2026 Census in accordance with the relevant Records Authority.</p> <p data-bbox="336 786 663 819">No further issues identified.</p>

5.4 Summary

IIS finds the ABS's collection of personal information about social media users in some limited circumstances to be reasonable and occurring in compliance with key privacy principles.

6. Digital service and myGov Census pathway

The Census Digital Service team works closely with the Census Customer Experience team. It is responsible for designing and developing the online Census form as well as the various self-service channels (e.g. request a paper form, contact the ABS). Similarly with the Customer Experience team, in the Phase 1 PIA the Digital Service team was in very early stages of planning. For Phase 2, the team informed IIS that it is making changes to some of the questions in the online Census form based on the Census content review and preparing a landing page ('page 1') for the Census which will go live ahead of the 2025 ORE; this will direct members of the public to the online Census form, or further help and support via self-service channels, or the Census website.

The team is also undertaking a series of changes to the non-functional components of the Digital Service, to improve security and performance. This includes standing up a new security operations centre (which will be available for the 2025 ORE and 2026 Census) and performance and penetration testing.

The ABS has engaged a new digital service vendor (Slalom) and a new address look-up provider (Intech). The address look-up service will not collect IP addresses.

6.1 Changes expected in 2026

The Digital Service team is anticipating the following changes for the 2026 Census:

- *Use of myGov as an additional Census pathway* – the team is exploring the use of myGov as a pathway to filling out the Census form.

6.2 Personal and other information involved

Personal information handled by the Census Digital Service team includes:

- Statistical information (Census) – collected via online Census forms.
- Personal information (members of the public) – collected via self-service (online) channels; typically, this includes name, contact details, address and the presenting issue/query.

myGov as a Census pathway

The ABS's exploration of the use of myGov as an additional pathway to the online Census form is in development. The proposal is for individuals to opt-in to receiving communications about the Census via myGov and as another pathway to completing the Census by authenticating through myGov.

For the 2025 ORE and 2026 Census Main Event the ABS will have a 3-week opt-in window which will provide the public the opportunity to subscribe to first complete the 2025 test and subsequently the 2026 main event Census via the myGov channel and to receive ongoing digital communication from the ABS. As part of the opt-in process, Services Australia will collect the individual's nominated Census night address. Those who subscribe will receive a 'save the date' reminder to their myGov inbox prior to the

Census collection period and a dedicated deeplink to the online form. The deep link will enable subscribers to bypass regular authentication processes.

myGov subscribers will be able to unsubscribe at any time. Depending on when an individual unsubscribes, physical mail will resume to the affected address.

In all cases, if an individual opts in via myGov, myGov will create a meaningless but unique identifier number (MBUN) linked to the nominated Census night address and provide both the address and MBUN to the ABS. No myGov profile data is shared with the ABS. The collected address is not stored in Services Australia systems.

The ABS will assign the MBUN to the address in its own internal systems and develop tailored communication and a deeplink. The MBUN allows these messages from the ABS to be directed to the individual's myGov inbox. As name has not been shared, all communication is without name.

When an individual opts-in to myGov, they are agreeing to a subscription service rather than creating a linked service in myGov. The person is agreeing to receive communications from the ABS via their myGov inbox. The person is also agreeing to sharing the Census night address with the ABS, so that the address is removed from the mail file which will stop the dwelling receiving physical mail. In effect this would mean reminders would be sent to the person's myGov inbox and possibly a deeplink or URL to the online Census form ahead of Census night. myGov users can opt-out at any time. At that point, the MBUN becomes invalid.

Digital service solution

Generally, the online entry point for the public is the digital service solution, which is housed by the ABS in an ABS tenancy within an AWS cloud platform. The digital service solution is the conduit via which individuals submit their online Census form or access online self-service channels (for example 'contact us' and forms for requesting a hard copy form). Information arrives in the digital service solution and is then transferred to the relevant downstream system – for example, the Scaled Analytical Data Environment (SADE) processing environment for completed online Census forms or the Census Agent Tool (CAT) for customer self-service queries.

These arrangements are the same as for the 2021 Census with third party provider Slalom engaged to deliver the Census digital service solution. The ABS advised that the AWS account is an ABS account and that Slalom will work within ABS systems. Automatic processes delete data from most digital service stores after transmission. Deletion of all other stores is done manually after completion of the overall census event. The digital service will then be decommissioned after the Census in December 2026.

6.3 APP analysis and other privacy risks

IIS has given particular attention in our APP analysis to those processes that will be different or new in 2026. With regard to use of myGov, we have analysed the data flows assuming that the ABS collects the Census night address of the individual. Collection and handling of the MBUN only is unlikely to be

covered by the APPs as it is unlikely to meet the definition of personal information in isolation. Even with collection of address by the ABS, we find that privacy risks are low due to the minimal information exchanged with Services Australia (which operates the myGov platform). Our analysis found that key APPs applying in this case include APPs 3 (Collection), 5 (Notice), 6 (Use and disclosure) and APP 11 (Retention).

We also give brief consideration to the separate issue of storage of data in the digital service solution (see last row of the table). This analysis concerns the digital service generally and not the myGov Census pathway.

APP	Comments and analysis
APP 3	<p><i>ABS collection of address and MBUN via myGov</i></p> <p>When an individual opts in via myGov to the ABS’s subscription service, they would provide the address they nominate being at on Census night which would be transmitted to the ABS along with an MBUN to enable the ABS to remove that address from the mail file, where applicable, to prevent physical mail being sent to the dwelling. The purpose of collection is to enable the ABS to provide the individual with a means of securely and efficiently accessing the online Census form. IIS finds this meets APP 3.1 – collection of the information (in this case, the individual’s address) is directly related to the ABS’s functions and activities. The collection also meets APPs 3.4 and 3.5, being fair and lawful and being directly from the individual.</p> <p>No further issues identified.</p>
APP 5	<p><i>Privacy notice for myGov</i></p> <p>The ABS is still at an early point in establishing arrangements for myGov. In line with APP 5, it should ensure the individual receives privacy information – preferably at the point at which the individual opts in to myGov. (This information could be included in a consent screen or in a terms of service statement but should be clear and straight-forward, not legalistic or buried in a long, complex notice.) The privacy information should make clear any additional uses beyond the Census (e.g. for household surveys) and, to enhance individual choice and control, the notice should also explain that the individual may opt-out at any time. The information provided to the individual when they opt in could also explain that by opting in to receiving messages via myGov, the individual will receive a link to the online Census form rather than a hard copy form in the post.</p> <p>There is no additional APP 5 obligation to notify others in the same household that the individual has opted in to notifications via myGov. However, the ABS may have other non-privacy related considerations in relation to managing multi-person households where one person has opted in to the myGov subscription. IIS understands that the ABS plans to make clear to individuals when they opt in that they will be responsible for filling out the Census form on behalf of their household and should let the others know.</p>

APP	Comments and analysis
	<p>(Note that a privacy notice will not be necessary if the ABS collects only the MBUN with no additional information.)</p> <p>See Recommendation 2.</p>
APP 6	<p><i>Use of information connected to myGov subscription</i></p> <p>IIS understands that the primary use of the individual’s address and MBUN in relation to myGov is to provide the individual with a means of securely and efficiently accessing the online Census form. This complies with APP 6.1. A related secondary use is to remove the individual’s address from internal mailing lists for physical forms. IIS finds that this is a logical secondary use that is likely to be anticipated by the individual – particularly if the APP 5 privacy notice makes clear that, by opting in, the individual agrees to receiving Census communications via their myGov inbox rather than via the physical post. This therefore would appear to align with APP 6.2(a).</p> <p>Other uses closely connected to this one include adding the individual’s address back into internal mailing lists for physical forms if the individual opts-out of myGov prior to the Census and sending the individual a receipt or reminder after Census night. We find these uses fall within APP 6.1 or 6.2(a).</p> <p>The ABS has indicated that it may use the myGov link as a conduit for household surveys also (following a similar approach as with the Census). If the ABS makes this use clear up front in the privacy notice – i.e. that by opting in, the individual agrees to receiving communications about the Census and other household surveys via their myGov inbox, IIS finds that this secondary use is likely to meet APP 6 – either the use could be classed as a primary use (APP 6.1), or a secondary use within reasonable expectations (APP 6.2(a)) or a secondary use with (implied) consent (APP 6.1(a)). The fact that the individual may opt out at any time from the subscription service further reduces the privacy impact of this arrangement.</p> <p>It was not clear to IIS at the time of writing how this opt-out mechanism would work in practice. The ABS advised IIS that Services Australia (the agency that operates myGov) is currently building the myGov subscription service which would manage all of an individual’s subscriptions. IIS understands that this will include a dedicated subscription menu which myGov users can use to opt out of their subscription to the ABS.</p> <p>No further issues identified.</p>
APP 11	<p><i>Storage and retention of address and MBUN in connection to myGov</i></p> <p>If the ABS decides to use the myGov pathway for other household surveys, this will necessitate retention of address and MBUN information to enable ongoing communication via myGov. The ABS advised IIS that the MBUN would be stored in the EMI alongside the address the individual uses to opt in via myGov. The Census Digital Service will also store the MBUN and will use this to pass information back and forth between the Services</p>

APP	Comments and analysis
	<p>Australia and ABS backends. The storage of this information in the EMI and Census Digital Service, will therefore be subject to the security arrangements applying to those systems. The ABS informed IIS that the MBUN would be retained in the Census Digital Service for the duration of the enumeration period and that the MBUN and address may be retained in the EMI for longer, depending on what ongoing engagement the individual has consented to.</p> <p>With clear specification of the primary and secondary purposes of collection, this retention is likely to be permissible under APP 11.2. Further, the ABS has made clear that when an individual opts-out, the MBUN becomes invalid, at which point, presumably, the individual's address or related information is removed from the ABS's myGov lists.</p> <p>No further issues identified.</p>
Other risks	Comments and analysis
APP 11	<p><i>Temporary storage of data in the digital service solution</i></p> <p>IIS reviewed the data flows associated with the digital service solution. The digital service solution and associated data flows are very similar to arrangements in 2021. That said, IIS did, during its analysis, inquire into how long data remains in the digital service solution once the data has been transmitted to downstream systems such as SADE and CAT. (APP 11 requires reasonable steps to safeguard personal information and secure disposal of the information when no longer needed.)</p> <p>The ABS advised IIS that most data will be automatically deleted from the digital service solution once safely received in downstream systems. Any data remaining in the digital service after the Census event will be manually deleted. The digital service solution will then be decommissioned after the Census in December 2026. Moreover, the digital service solution can expand its storage of data as needed if, for example, there is a problem with a downstream system which provides necessary 'give' in the overall information architecture. In the digital service solution, data is encrypted at rest and in flight.</p> <p>No further issues identified.</p>

6.4 Summary and recommendations

By our analysis, the privacy impacts associated with use of myGov as a Census pathway appear to be low – risks are further reduced by the privacy preserving features of myGov itself. IIS also notes that Services Australia is also conducting a PIA on the myGov subscription functionality. Our recommendation, therefore, is limited to ensuring compliance with APP 5. That said, the ABS's work on a myGov proof of concept is still in development and may benefit from a further check, if arrangements change or develop further. This may be something for the Phase 3 PIA to revisit.

Recommendation 2 – Ensure myGov privacy information makes clear possible additional uses of myGov by the ABS beyond the Census

Compliance recommendation

Provide individuals with privacy information (in accordance with APP 5) at the point at which the individual opts-in and consents to receiving Census communications via myGov. Ensure the privacy information makes clear any additional uses of myGov beyond the Census (e.g. for household surveys) and, for reasons of best practice, make clear that the individual may opt-out at any time.

7. Coverage and data quality

The Coverage and Data Quality team is responsible for maintaining accurate dwelling counts and coverage based on the ABS Address Register as well as Census field operation intelligence. The team is also responsible for implementing processes to ensure data quality throughout the enumeration and processing stages.

The purpose for collecting and using the address information is to reconcile forms against the Census frame to ensure that the ABS does not have duplicate or missed dwellings and to ensure that it has counted dwellings in the right spot.

7.1 Changes expected in 2026

IIS understands that only a very minor change is envisaged for 2026:

- *Use of front-of-form address to update address frame data on the Enumeration Management System (EMI)* – The so-called front-of-form address (i.e. the address the person was at when they filled out the Census form) has always been used to process and reconcile dwellings during enumeration. The change, this time around, is the use of front-of-form addresses to create entries where the reconciliation team has determined the dwelling does not already exist on the address frame (in the EMI). These new entries could then be provided to the Address Register team to determine whether they should be added.

7.2 Personal and other information involved

In performing its functions (e.g., reconciling dwellings, creating new unit dwellings), the team uses address information from the following sources:

- Address Register
- Paper form requests that come via the contact centre or digital services channels
- Annotations created by field officers
- Online self-service (i.e., address provided by a person as part of the process to access the online Census form)
- The Census night address provided in the Census form itself.

A core consideration is whether, when separated from any associated personal information (e.g. name, Census form information, Census self-service query information etc), addresses meet the definition of 'personal information' and therefore trigger the coverage of the APPs. In our view, use of address information in isolation will generally not be personal information.

7.3 APP analysis and other privacy risks

The use of front-of-form addresses to update the address frame on the EMI raises the threshold issue of whether the information qualifies as personal information and therefore whether the APPs apply to its

handling. This matter is discussed in the table that follows, along with possible additional best practice considerations in relation to ensuring clarity on ABS use of address information.

<i>APP</i>	<i>Comments and analysis</i>
Definition of PI	<p><i>Front-of-form address information and the definition of PI</i></p> <p>Once the front-of-form address has been removed from other identifying information to enable use in updating the EMI address frame, IIS finds that the address information is unlikely to meet the definition of personal information as set out in the Privacy Act. Given the address frame is used to enable enumeration Australia-wide, there is no significance to an address being included in the frame.</p> <p>This contrasts with a situation where, for example, an address was added to a register of single-person households – in this case, the address may meet the threshold of personal information because inclusion in the register tells you something about the resident, and this combined with an ability to match with other datasets may render the information ‘personal.’ That is not the case here. Therefore, we find the Privacy Act and APPs are unlikely to apply to this activity.</p> <p>No further issues identified.</p>
<i>Other risks</i>	<i>Comments and analysis</i>
Public misunderstanding	<p><i>Retention of address information</i></p> <p>The ABS disposes of Census address information no later than three years after Census night in accordance with its Records Authority 2021/00429564. The 2021 Census Privacy Notice made this retention period clear, though also contained some additional information about how the ABS used address information and other projects involving use of address information. From reviewing the 2021 Notice, it would appear that the proposed use of front-of-form address information to update the address frame would broadly fall within the terms of the notice.</p> <p>IIS suggests only that the ABS review its 2026 Privacy Notice (when available) to ensure information about collection and retention of address information is clear and not confusing (see Recommendation 9).</p> <p>No further issues identified.</p>

7.4 Summary

In our view, the privacy risk associated with this proposed use of address information is low given our understanding that the information is unlikely to meet the definition of personal information. This also means that the APPs are unlikely to apply in this case. We also find that the proposed use is closely associated with the uses the ABS already makes of address information for validation and reconciliation purposes.

That said, given commitments given in the Census Privacy Statement about retention of address information, IIS suggests (for reasons of transparency and best practice) that the ABS review the proposed privacy statement for the 2026 Census (and any other relevant information contained on the Census website) to ensure nothing in the statement contradicts the ABS's planned uses of address information (including front of form information). We also suggest the ABS make clearer what it means for the ABS to state that it disposes of address information no later than 36 months while also retaining address information for use in other projects. See **Recommendation 9**.

8. Data design and WoAG Coding Capability

The Data Design team is responsible for developing the systems and workflows that process the data contained in completed Census forms. The processing stage involves both automated and manual coding of data. The team informed IIS that for the 2021 Census, at its peak there were up to 600 people working on manual coding. Changes described below should further automate the process and reduce the number of people needed for manual coding.

8.1 Changes expected in 2026

The Data Design team is anticipating the following changes for the 2026 Census:

- *New processing systems* – the ABS's new Scaled Analytics Data Environment (SADE) will shift Census data processing and storage from legacy on-premises systems to storage in an ABS tenancy within a secure, certified cloud-based hosting; this will allow classification of Census data as PROTECTED.
- *Development and deployment of the Whole of Australian Government (WoAG) Coding Capability* – the Coding Capability will use machine learning to code input text (i.e. survey response data) against statistical classifications and will initially be used in relation to seven Census topics: Occupation, Industry, Language, Ethnicity, Religion, Education and Country of Birth.
- *Development of a 2026 Census Synthetic Test Dataset* – the synthetic dataset would allow the ABS to more efficiently and effectively test the next Census cycle's systems. The purpose of the test dataset is to enable effective testing of processes for matching and linking between the Census, Post Enumeration Survey, Frame reconciliation, and address coding.

8.2 Personal and other information involved

In performing its functions, the Data Design team handles the following information:

- Statistical information (Census) – collected via Census forms.
- De-identified data – de-identified coded datasets from the 2021 Census are being used to train models used by the Coding Capability, de-identified uncoded datasets from the 2016 Census are then used to test the models.
- Synthetic data – synthetic names and addresses used in combination with analytic data from the 2021 Census to develop a test dataset which allows teams to test and evaluate systems and processes for the 2026 Census.

New processing systems

The 2026 Census processing systems are undergoing a major redesign for the 2026 cycle. The uplift of the systems will shift Census data processing and storage from legacy on-premises systems to the ABS's SADE – a secure, certified cloud-based AWS environment.

SADE is not a Census-only system and is already operational within the ABS for other use cases. For example, it is used to process administrative data from the ATO pertaining to Single Touch Payroll to inform Weekly Payroll Jobs and Wages statistics. However, this will be the first time SADE has been used for the Census. Census data will be segregated from other ABS data within SADE.

Development of WoAG Coding Capability

The ABS is developing a Whole of Australian Government Coding Capability (also known as the WoAG Coder). While the WoAG Coder will improve coding of Census data, its scope is broader than the Census with a goal of being made available to other government agencies and registered users – that is, other agencies outside the ABS will eventually be able to use the tool to code their own data and datasets. Users of the WoAG Coder will have access to the tool but not to any Census data. They will submit their data (e.g. uncoded occupation data) and the tool will return the data with an official ABS standard occupation code and title.

Coding of Census data has always occurred. Foundationally, it simply means converting raw data – e.g. a person's response of 'Church of England' to a question about their religion – into the agreed generic descriptor – e.g. 'Anglican' – so that responses of Anglican, Church of England, C of E and misspellings of these responses are all counted as 'Anglican.' This is done with a combination of manual and automated processes. In the past, automated coding was deterministic. That is, programmers specifically told the model to convert 'Church of England' to 'Anglican.' The WoAG Coder will make that automated process more sophisticated by using probabilistic models and large language models (LLM). Instead of having to program in each variation the WoAG Coder can learn variations and likely variations through use of a large language library (in this case, DistilBERT) and exposure to existing datasets that have already been coded.

Once the models have been trained on pre-existing coded datasets from 2021, the resulting output (a machine-readable file) can be used to code other input data. The team is planning to perform a re-code of 2016 Census data to assure the models impact on Census output data quality. It will then conduct a bigger test of the models during the 2025 ORE.

Development of a 2026 Census Synthetic Test Dataset

The development of a Census Synthetic Test Dataset is aimed at creating a persistent testing resource for the 2026 Census and beyond using 2021 Census response data with synthetic names and addresses. This will result in a large, complex testing dataset which will allow Census teams to test systems and processes with realistic data while maintaining the privacy of respondents.

The ABS has undertaken three PTAs for this project covering: creation of synthetic names; creation of synthetic addresses; and use of raw analytic data from the 2021 Census. In setting out the case for a testing dataset, the PTAs note that during the development and testing phase for Census 2021, many teams did not have access to test data that would allow them to test and evaluate the systems, processes, and edits they were developing. Individual teams handcrafted test data for their own specific purposes which was resource intensive and often could not provide the volume, variation and relationships that would be found in production data. Hence, this project aims to generate a synthetic test

dataset that mimics the size and variation of production data, thus allowing system testing to begin earlier and more effectively, potentially allowing end-to-end testing to take place independently of and prior to large scale field tests like the ORE.

The Synthetic Test Dataset uses analytic data from the Census 2021 merged with synthetic names and addresses. Real names and addresses are removed and there is no ability to link the data to the correct original names and addresses. The Census Synthetic Dataset will be stored in SADE.

8.3 Stakeholder feedback

A major theme of the feedback from stakeholders on the Coding Capability was the potential for public perception risks, and possible negative associations with AI and machine learning (ML). For this reason, IIS suggests that the ABS publish explanatory information about the Coding Capability on its website (this is discussed further in the analysis below).

8.4 APP analysis and other privacy risks

IIS has given particular attention in our APP analysis to those processes that will be different or new in 2026. Regarding the Census Synthetic Test Dataset – while this will be a new element during the lead up to the 2026 Census, it has already been the subject of three PTAs on creation of synthetic names, creation of synthetic addresses, and use of analytic Census data respectively. IIS reviewed those PTAs and was satisfied with the process the ABS followed to assess the project for possible privacy risks. IIS also notes that the Test Dataset will comprise synthetic and therefore non-personal information which will move it outside the scope of the APPs. Moreover, development of a Test Dataset may enhance data quality by allowing more effective testing of processes to match and link Census data with Post Enumeration Survey Data.

Therefore, the APP analysis set out in the table below is primarily concerned with the WoAG Coder. There are two aspects to the analysis – first, use of Census data to train the models that will underpin the WoAG Coder; and second, the use of the WoAG Coder to code Census 2026 data. Regarding the first item, we find that the APPs are unlikely to apply because the data being used to train the models is de-identified. Regarding the second item, though the data processed through the coder is de-identified, we have opted to apply the APPs for reasons of best practice – key APPs relevant to this case include APPs 5 (Notice), 6 (Use and disclosure) 10 (Data quality) and 11 (Security). Wider use of the WoAG Coder by other authorised users is out of scope for this PIA.

APP	Comments and analysis
Definition of PI	<p><i>Data used to train WoAG Coder</i></p> <p>The team developing the WoAG Coder is training the models that will underpin the Coder using de-identified data from the 2021 Census. Initially, the coder will be used to code seven Census topics: Occupation, Industry, Language, Ethnicity, Religion, Education and Country of Birth. In practice, this means that Census 2021 responses for each topic are separately extracted with synthetic row count numbers as the unique ID for the data. The</p>

APP	Comments and analysis
	<p>Person_ID field is not extracted to prevent matching back to either the original Census 2021 data or to other topic datasets used to train the models. The team will then test their models on de-identified uncoded 2016 Census data.</p> <p>No Census data leaves ABS systems or environments during the training of the models and Census data is not used at all in the resulting tool used for coding other datasets. The ABS advised IIS that no personal information was used during model training – rather models were trained using de-identified unit record Census data which is transferred from the Census NGI into AWS (S3 bucket) for this purpose.</p> <p>This use of de-identified data to train the models that underpin the WoAG Coder falls outside the operation of the APPs which apply to personal information only.</p> <p>Use of the WoAG coder to code 2026 Census data may also fall outside the operation of the APPs because the response data is separated from all other unrelated response data, de-identified and given an independent synthetic identifier prior to coding. At no point does the coder process identifiable Census data. However, given that this is broadly a ‘use’ of live 2026 Census data (albeit an extremely safe use involving de-identified data), we have opted to apply the APPs anyway, for reasons of best practice. As is clear from the analysis that follows, use of the coder appears to meet APP requirements.</p> <p>No further issues identified.</p>
APP 5	<p><i>Notice obligations in relation to WoAG Coder</i></p> <p>APP 5 requires an agency to notify individuals of certain information (outlined in APP 5.2) when it collects personal information about the individual. IIS reviewed APP 5.2 and finds that none of the provisions require the ABS to notify individuals of its approach to coding Census response data. However, from a best practice standpoint and to foster transparency and social acceptance, the ABS should publish some information about the WoAG coder and how it is used in conjunction with the Census. This is discussed further below.</p> <p>Regarding APP 5 compliance, no further issues identified.</p>
APP 6	<p><i>Use of WoAG Coder to code Census data</i></p> <p>The ABS’s use of the WoAG coder to code Census data can be considered a ‘use’ for the purposes of APP 6. IIS finds that coding of response data forms a foundational part of the primary purpose of collection of statistical information by the ABS. We also find that this is not a new use of the information. In this case, it is only that the technology used for coding has changed. While this may have other privacy or security implications, it does not appear to change the application of APP 6.</p> <p>No further issues identified.</p>

APP	Comments and analysis
APP 10	<p><i>Data quality in relation to WoAG Coder outputs</i></p> <p>APP 10 requires an agency to take reasonable steps to ensure the information it uses, having regard to the purpose of the use, is accurate, up-to-date, complete and relevant. The use of Census information for statistical purposes is relevant to the interpretation of this principle. Given that there is no direct impact on the individual regarding inaccurate Census information, the privacy impact is significantly reduced. So the steps that are 'reasonable' for the purposes of APP 10 might be lesser than in a case where inaccurate information may have a direct, adverse impact on an individual.</p> <p>IIS finds, therefore, that steps to ensure data accuracy will be driven by statistical objectives (i.e. ensuring data used in the production of statistics is accurate) rather than privacy ones (i.e. ensuring data used in decision-making about an individual is accurate).</p> <p>The ABS advised it has measures in place to ensure a high degree of data accuracy. In relation to the performance of the models that underpin the Coder, this includes managing drift of the model over time through retaining the de-identified training data to allow monitoring of model lineage and track data changes. In relation to the actual coding of Census data, this includes setting a confidence threshold for coded data where data falling below the threshold is referred to a human for manual review.</p> <p>No further issues identified.</p>
APP 11	<p><i>Security considerations in relation to WoAG Coder and associated data processing</i></p> <p>APP 11 requires an agency to take reasonable steps to safeguard the personal information it holds. The ABS advised that instances of ML in connection with the training of the models that underpin the WoAG Coder occurs in ABS-owned AWS accounts only. Training occurs within a secure S3 bucket in AWS. Once models are trained, they are placed in a separate PROTECTED-level security account for coding.</p> <p>In coding Census data, the response data is de-identified and separated from all other unrelated topic (response) data, and then given an independent synthetic identifier. The output of the WoAG Coder is constrained to predetermined classifications (that is, it is not generative). The ABS advised that there is no external connection used during the coding process (that is, no training and/or production data ever leaves ABS's AWS accounts).</p> <p>No further issues identified.</p>
Other risks	Comments and analysis
Public misunderstanding / loss of	<p><i>Possible public concern over ABS use of ML and LLMs</i></p> <p>Consultations with external stakeholders regarding ABS development and use of the WoAG Coder revealed some concerns over ABS use of ML and LLM. IIS suggests that, in the interests of transparency and reducing the likelihood of public misunderstanding, the</p>

<i>APP</i>	<i>Comments and analysis</i>
trust	<p>ABS publish explanatory information on its website about how it codes Census data and the measures in place to ensure coding happens safely and securely.</p> <p>See Recommendation 3.</p>

8.5 Summary and recommendations

IIS finds that the ABS’s development and deployment of the WoAG Coder, in relation to the Census, complies with the APPs. The ABS is taking a cautious approach and has appropriate controls in place to manage privacy risks and safeguard data, both during testing and use during the Census.

One risk IIS identified during analysis and consultation with external stakeholders was a perception risk associated with possible public misunderstanding of the ABS’s use of ML and LLMs in connection with Census coding. To be clear, this is a risk of public misunderstanding, rather than data misuse or non-compliance. Currently, due to the recent rapid rise of a number of publicly available AI tools, there may be a heightened sensitivity in the community about the ABS’s use of ML or LLMs, notwithstanding the controls in place and low residual risk. We therefore recommend that the ABS publish information on its website explaining its coding activities as they relate to the Census.

Recommendation 3 – Publish explanatory information about Census coding on the ABS website

Best practice recommendation

Publish explanatory information on the ABS website about the ABS’s approach to coding Census data and the WoAG Coder. The purpose of publishing this information would be to enhance transparency, encourage trust and social acceptance and reduce the possibility of public misunderstanding.

9. Use of administrative data

As with the 2021 Census, the ABS intends to use administrative data to improve certain Census outcomes. However, some changes in approach are anticipated for 2026.

Administrative data is information collected by government agencies, businesses or other organisations for various purposes, including registrations, transactions and record keeping, usually during the delivery of a service. The ABS receives administrative data from third party data custodians for statistics and research purposes. This PIA assesses two proposed uses of administrative data described below.

9.1 Changes expected in 2026

The ABS anticipates the following changes for the 2026 Census:

- *Use of administrative data to assist with determinations of Census-night dwelling occupancy* – the ABS proposes to use certain administrative datasets to create a statistical model to assist in determining if a house was unoccupied during the Census collection period and does not require additional follow up visits, thus improving efficiency of operations. (Use case 1.)
- *Use of administrative data to fill in some missing data about non-responding households* – the ABS proposes to use administrative data to create records for occupants of dwellings that did not return a Census form. Administrative data would be used to directly impute data relating to house type, persons per household, age, sex, marital status and Indigenous status (subject to community consultation). (Use case 2.)

These changes build on similar administrative data use cases from the 2021 Census. Regarding use case 1, in 2021 administrative data was used only after the Census collection period to help determine whether a house was unoccupied, and some administrative datasets (e.g. energy usage) were area level. In 2026, use case 1 will also occur during the collection stage to enable more efficient follow-up, and some extra administrative datasets are proposed to be used, including at the dwelling level (see below).

Regarding use case 2, in 2021 administrative data was used to assist in selecting a similar 'donor' household for those households that did not return a form, whereas in 2026 the ABS will use administrative data more directly for imputation. This is intended to achieve a more accurate population count.

9.2 Personal and other information involved

Regarding use case 1, the ABS proposes using the following dwelling-level administrative data:

- Electricity usage
- Rentals
- Solar panel installation

- PLIDA activity (i.e. transaction data relating to Medicare, Centrelink, Australian Taxation Office, Address register)
- 2021 Census.

Regarding use case 2, the ABS proposes using administrative data sourced from PLIDA to impute the following information for households that do not return a form:

- House type
- Persons per household
- Age
- Sex
- Marital status
- Indigenous status (subject to community consultation).

Regarding use case 1, the ABS advised IIS the administrative data in question may be brought into the ABS under a wider multi-use agreement (allowing other uses of the data for other purposes beyond the Census) or may be brought in just for the Census. Where a wider multi-use agreement is used, this would be subject to a separate privacy governance process (which would likely include a PTA and possible PIA).

9.3 Stakeholder feedback

Concerning use case 1, some stakeholders who participated in the roundtable questioned whether the collection of the proposed administrative data would be within the reasonable expectations of the people that provided their data (or had data about them collected) in the original context. Stakeholders reinforced the importance of communication as to how the data will be collected and used. Two stakeholders noted that it would be important to highlight that the data would not be used for regulatory and compliance purposes – IIS notes that this was a recommendation of the 2020 administrative data PIA and was implemented by the ABS ahead of the 2021 Census.

Concerning use case 2, stakeholders raised some similar concerns as in relation to use case 1 – in particular the privacy impact of using administrative data originally collected for one purpose for an unrelated secondary purpose (imputing data into the Census) – and the likelihood that this would be outside individuals' reasonable expectations. There were also comments, during the roundtable concerning extraction and use of unit-level PLIDA data and whether this aligned with the purpose of PLIDA. In their view, unit-level data goes into PLIDA but generally the use of PLIDA data is in the aggregate – the direction of unit-level to aggregate should be 'one-way'.

We also received feedback suggesting the ABS engage in white hat testing of the re-identifiability of dummy data to strengthen arrangements in place to minimise misuse and re-identification. White hat testing may be relevant for more than just Census projects involving administrative data. Other Census activities involving use of ostensibly de-identified data may benefit from such testing. It was not clear to

IIS at the time of writing whether the ABS already plans to undertake testing of this sort. This may be something that can be explored further in the Phase 3 PIA.

9.4 APP analysis and other privacy risks

IIS assessed the ABS’s proposed use of administrative data in the Census in the Phase 1 PIA. In that PIA, IIS applied broad principles of good privacy and best practice. In doing so, IIS recommended that the ABS formally consider whether the proposed use of administrative data to determine Census night occupancy and the intrusion on individual privacy was justified and proportionate to the anticipated benefits. IIS also recommended the ABS formalise rules on the use of administrative data for use case 1 (guided by the principles of data minimisation, purpose specification and use limitation) and develop communication material to explain administrative data use.

In this PIA, we have given a closer assessment under the APPs, set out in the table below. We find that the relevant APPs in this case include APPs 3 (Collection), 5 (Notice), 6 (Use), 10 (Data quality) and 11 (Security and retention).

Note that APP 3 largely applies to use case 1 which involves collection of administrative datasets, while use case 2 involves use of PLIDA data which, though subject to approval processes for its use, is already held by the ABS. The ABS is the Accredited Integrating Authority for PLIDA. While this restricts the ABS’s use of PLIDA data to those uses formally reviewed and authorised under PLIDA governance arrangements, the APPs treat handling of the data (for example, for use case 2) as a ‘use’ rather than a ‘collection and use’ because the ABS already ‘holds’ the data, for the purposes of the Privacy Act.

APP	Comments and analysis
Definition of PI	<p><i>Whether use case 1 administrative data is personal information</i></p> <p>The ABS proposes collecting and using a number of population-wide administrative datasets (set out above) for use case 1. This information will be dwelling level information and the data will be handled in an unidentified form with linkage variables (in this case, addresses) separate from analytic variables (e.g. electricity usage, PLIDA transactions etc).</p> <p>It was difficult to determine whether the administrative data in question met the threshold for being ‘personal information’ for the purposes of the Privacy Act. The controls in place to separate data and to handle it in anonymised form (via encoding of addresses and hashing) make the risks of re-identification of the dataset low. That said, decoding of addresses is necessary to the purpose of use case 1 (enabling targeted follow-up) and so this may meet the ‘reasonably identifiable’ limb of the Privacy Act definition of personal information, albeit in only very limited stages of the information lifecycle.</p> <p>The fact that the information is at an address level rather than a person level does not change this. For single person households, information about energy usage and other indicators can be considered information about the individual. For multi-person</p>

APP	Comments and analysis
	<p>households, information about energy usage is still information about each inhabitant of the household, even if that information is the same for each inhabitant.</p> <p>In our view, where there is uncertainty about ‘identifiability,’ it is worth treating the information as if it were ‘personal information’ and applying the APPs accordingly. (We believe the ABS is doing this, and we find that the ABS has strong controls in place to minimise re-identification.) We have therefore taken a cautious approach and applied the APPs to use case 1 in the analysis that follows.</p>
Definition of PI	<p><i>Whether use case 2 administrative data is personal information</i></p> <p>IIS understands that the ABS will use PLIDA data to fill in high level information for non-responding households. As with use case 1, IIS understands that the ABS will handle PLIDA data largely in anonymised form and in accordance with functional separation principles. However, person-level processing will be necessary to enable imputation of the variables mentioned and to allow de-duplication. Therefore, our view is that the data to be used in use case 2 can be considered personal information, even while being processed largely in un-identified form. To the extent this data meets the personal information threshold, it is covered by the APPs.</p>
APP 3.1	<p><i>Collection of administrative data for use case 1</i></p> <p>When entering into a data arrangement with the ABS, data custodians must specify the legal authority under which they disclose the data. Where required, the ABS may issue a Notice of Direction under the Census and Statistics Act to provide the custodian with legal authority to disclose. The ABS’s data arrangements are governed by its ‘Data Acquisition under the Census and Statistics Act Policy,’ its ‘Paying for Data Policy’ and its ‘Memorandum of Understanding and Other Partnership Arrangements Policy.’</p> <p>APP 3 allows an agency to collect personal information if the information is directly related to one or more of the agency’s functions or activities. IIS finds that the ABS’s collection of administrative data to determine Census night occupancy meets this requirement. IIS further notes that administrative data may be collected under a wider data-use agreement allowing other uses of the data. Here, we have focused on use of the data for Census-night occupancy determinations – other uses are out of scope for this PIA.</p> <p>No further issues identified.</p>
APP 3.5	<p><i>Collection of administrative data for use case 1 is fair and lawful</i></p> <p>APP 3.5 requires that an agency only collect personal information by fair and lawful means. IIS finds that the ABS’s collection of administrative data for use case 1 meets the lawful limb of this principle. Regarding fairness, the OAIC advises that a ‘fair means’ of collecting information is one that does not involve intimidation or deception, and is not</p>

APP	<i>Comments and analysis</i>
	<p>unreasonably intrusive.⁷ The OAIC further advises that, depending on the circumstances, ‘it would usually be unfair to collect personal information covertly without the knowledge of the individual.’⁸</p> <p>The ABS has no intention of hiding its collection and use of administrative data for use case 1. That said, its challenge is to ensure its collection and use is overt and clear to the public in circumstances where the public may not otherwise be aware of the collection, given that the collection occurs indirectly and involves data that was originally collected for an unconnected purpose.</p> <p>In order to ensure collection of the administrative data occurs by fair means, the ABS should notify individuals of its administrative data activities and test the effectiveness of awareness raising activities. IIS also notes its recommendation in the Phase 1 PIA that the ABS formally consider whether the proposed use of administrative data to determine Census night occupancy and the intrusion on individual privacy was justified and proportionate to the anticipated benefits. In addressing that recommendation, the ABS could also consider the ‘fairness’ requirement under APP 3.5 and the OAIC’s advice that collection should not be unreasonably intrusive.</p> <p>See Recommendations 4 and 5.</p>
APP 3.6	<p><i>Collection of administrative data for use case 1 from sources other than the individual</i></p> <p>APP 3.6 requires an agency to collect personal information directly from the individual unless an exception applies. Exceptions include where the individual consents to indirect collection; where the agency is required or authorised by law to collect the information indirectly; or where direct collection would be unreasonable or impracticable. IIS finds that the ABS’s collection of administrative data from data custodians is likely to meet both the ‘authorised by law’ and ‘unreasonable/impracticable’ exceptions.</p> <p>While the ABS may meet the requirements for APP 3.6, IIS suggests the ABS test public awareness and understanding of administrative data collection, to counter the privacy impact of the information being collected indirectly and without consent.</p> <p>See Recommendation 5.</p>
APP 5	<p><i>Privacy notice obligations in relation to administrative data use (use case 1)</i></p> <p>APP 5 requires an agency to notify an individual of certain information when it collects personal information about the individual. The ABS included information about its collection and use of administrative data in its Census 2021 Privacy Statement. The Statement included a link to more detailed information.</p>

⁷ OAIC, *APP Guidelines*, paragraph 3.62.

⁸ OAIC, *APP Guidelines*, paragraph 3.62.

APP	Comments and analysis
	<p>Given that the range of administrative datasets that the ABS will collect will expand in 2026 and the fact that these datasets will be at the dwelling and, at times, person level rather than mesh-block level, the ABS should include specific information in the Census 2026 Privacy Statement about the administrative data it will be collecting and the purpose of collection. APP 5.2(b) is particularly relevant as it applies to cases where an agency is collecting information indirectly or where the individual may be unaware of the collection. In such circumstances, an agency must notify the individual or otherwise make them aware of the fact that the agency so collects, or has collected, the information and the circumstances of that collection. See Recommendation 4.</p>
APP 6	<p><i>Use of administrative data for use case 1</i></p> <p>The ABS will use administrative data collected for use case 1 to assist with determining Census-night occupancy, both during and after the Census collection period. IIS understands that this will involve isolating non-responding addresses in the datasets, applying formulas to the data to flag addresses that may have been unoccupied on Census night and integrating administrative datasets from respective data custodians to enhance the accuracy of an occupancy determination. IIS further understands that processing involves applying strict data separation, working with unidentified data, encoding of addresses and hashing.</p> <p>After – and separate to – that process, administrative data about occupied non-responding households will be used to support imputation in connection with use case 2.</p> <p>APP 6 states that personal information must only be used for the primary purpose it was collected unless an exception applies. IIS finds that the proposed data processing outlined above falls within the primary purpose of collection and therefore meets APP 6. Where the ABS acquires the administrative data under a multi-use agreement, as long as use of the data for Census occupancy determination is specified as one of the permitted uses in that agreement, this is still likely to be considered use for (one of) the primary purpose(s) of collection rather than a secondary use. Or, if considered a secondary use, that use would likely be permitted by the ‘required or authorised by law’ exception under 6.2(b). Secondary use of the data to test occupancy models for the following Census cycle (Census 2031), is also likely to be permitted by APP 6.2(b).</p> <p>Certain aspects of use case 1 and the administrative data involved increase the associated privacy risks. This includes:</p> <ul style="list-style-type: none"> ● the amount and richness of the data ● the fact that the data was initially collected for an unrelated purpose ● the fact that data will be collected indirectly ● the fact that some sources of administrative data have not been collected by the ABS previously

APP	Comments and analysis
	<ul style="list-style-type: none"> ● the likelihood that collection may be outside individuals' reasonable expectations ● the possibility (due to indirect collection) that individuals may be unaware of the data collection and use. <p>These factors increase the privacy risk. Therefore, IIS has opted to formalise use limitation in a recommendation to reassure the public that the ABS will limit secondary use. See Recommendation 6.</p> <p><i>Use of administrative data for use case 2</i></p> <p>The ABS proposes to use PLIDA data to fill in basic information (house type, persons per household, age, sex, marital status, Indigenous status) for occupied non-responding households to assist with ensuring an accurate population count.</p> <p>As part of that process, the ABS will also use PLIDA data to de-duplicate individuals appearing twice in the dataset (for example, listed as an inhabitant of a non-responding household and included in the form of a separate responding household). De-duplication requires a data linkage process with PLIDA data involving name, date of birth and address.</p> <p>APP 6 states that personal information must only be used for the primary purpose it was collected unless an exception applies. Use of PLIDA data for this purpose could be considered a 'primary purpose' given that the data is collected for use in approved PLIDA research projects, of which use case 2 is one. If use of PLIDA data for use case 2 is treated as a 'secondary purpose,' that use is likely to meet the exception in APP 6 allowing a secondary use authorised by law – with the authorising legislation in this case being the ABS Act and the Census and Statistics Act. Those laws permit the ABS to undertake surveys and the Census, collect information from other data custodians and link Census data and other information. IIS also notes that PLIDA is subject to its own governance arrangements which includes a rigorous assessment and approval process for projects wishing to use PLIDA data. For a project to be approved the data custodians must agree to the proposed use of the data and the project must be assessed as being in the public interest.⁹</p> <p>Either way, APP 6 would appear to permit use.</p> <p>No further issues identified.</p>
APP 10	<p><i>Data quality and use of administrative data (use cases 1 and 2)</i></p> <p>APP 10 requires an agency to take reasonable steps to ensure the information it collects and uses, having regard to the purpose of the collection, is accurate, up-to-date, complete and relevant. The use of administrative data to support the Census and associated</p>

⁹ See ABS, [PLIDA/MADIP research projects](#).

APP	Comments and analysis
	<p>statistical purposes is relevant to the interpretation of this principle.</p> <p>Given that there is no direct impact on the individual regarding inaccurate Census information, the privacy impact is significantly reduced. So the steps that are ‘reasonable’ for the purposes of APP 10 might be lesser than in a case where inaccurate information may have a direct, adverse impact on an individual. IIS finds, therefore, that steps to ensure data accuracy will be driven by statistical objectives (i.e. ensuring data used in the production of statistics is accurate) rather than privacy ones (i.e. ensuring data used in decision-making about an individual is accurate).</p> <p>The ABS will rely, to some extent, on the data custodian providing the information to provide accurate data, but will also take steps (cleansing, integration with other datasets) which further improve data quality.</p> <p>No further issues identified.</p>
APP 11.1	<p><i>Security arrangements for administrative data (use cases 1 and 2)</i></p> <p>IIS understands that the ABS is still at an early stage of confirming specific internal data flows needed to support processing of administrative data for use cases 1 and 2. For example, different stages of data processing may take place in the Data Acquisition Centre, DataLab, SADE and the Data Linkage Centre. Each of these environments is already operational for data processing, linkage and analysis outside the Census and is subject to information security protections. Once the details of administrative data flows are formalised, a closer check of security arrangements may be conducted. We suggest those details be made available for assessment during the Phase 3 PIA.</p> <p>No further issues identified.</p>
APP 11.2	<p><i>Data retention arrangements for administrative data collected for use case 1</i></p> <p>The administrative datasets are to be used for the purpose of determining Census night occupancy. This activity supports targeted follow up (by field officers) of non-responding households and imputation for households that have still not returned a form by the end of the Census period. IIS understands this to comprise the primary purpose of collection of those administrative datasets (noting that there may be other purposes of collection if the information is acquired under a multi-use agreement).</p> <p>We further understand that the ABS intends to use the data in the lead up to the following Census (in 2031) to enable testing of occupancy models to be used in that Census cycle. This means that the ABS is likely to retain the information for at least five years. Where administrative data is brought in under a multi-use agreement, the information may be retained for longer or indefinitely, according to the terms of the agreement (though any additional uses permitted under a multi-use agreement are out of scope for this PIA).</p> <p>APP 11.2 requires an agency to destroy or de-identify personal information it no longer needs for the primary purpose of collection or a permitted secondary purpose. Exceptions</p>

APP	Comments and analysis
	<p>to this requirement include where the information is held in a Commonwealth record or where the agency is required by law to retain the information.</p> <p>IIS finds that the Commonwealth records exception is likely to apply in this case, which means that information retention is governed by the <i>Archives Act 1983</i> and the ABS's records authorities. Specifically, Records Authority 2021/00429564 applies to records documenting personal identifiers, such as names and addresses, collected or received from respondents or providers under relevant census and statistics legislation (currently ss 10 and 11 of the Census and Statistics Act) for the purposes of conducting the Census.</p> <p>The Records Authority requires the ABS to destroy those records as soon as practicable after the conclusion of data processing, but no later than 24 months after collection for names and 36 months after collection for addresses. This is the current relevant Records Authority. However, the ABS is developing a new Records Authority which will supersede all previous Authorities. The new Records Authority is currently with the National Archives of Australia for approval.</p> <p>We understand that the new authority will provide greater flexibility to retain records (in comparison to 2021/00429564 which is fairly prescriptive in requiring disposal of personal identifiers after specified periods of time). IIS understands that, while the new Records Authority will potentially offer greater flexibility, the ABS intends to maintain its policy of disposing of names and addresses collected in Census forms after 24 months and 36 months respectively, but that this policy will not apply to administrative data used for use case 1.</p> <p>In our view (and as explained above), the ABS's use of administrative data in this context involves some heightened privacy risks. For this reason, we have suggested that the ABS limit its use of this information, to the extent possible. During earlier analysis for this PIA, IIS suggested the ABS delete this information as soon as practicable after using it for determining occupancy for Census 2026 as this may reassure the community that data would not be used for unexpected secondary purposes. However, the ABS advised IIS that it may hold the data under a multi-use agreement, meaning that there may be additional uses which require the ABS to retain the information. The ABS further noted that the information would need to be retained for a minimum of five years to enable secondary use to test occupancy models for Census 2031.</p> <p>We are therefore recommending that the data be deleted from Census systems after five years. Use of the data for other non-Census purposes would be governed by the ABS's standard privacy governance arrangements and would, we understand, be the subject of a separate PTA / PIA process. Use of administrative data for non-Census purposes is out of scope for this PIA.</p> <p>See Recommendation 7.</p>

APP	Comments and analysis
Other risks	Comments and analysis
Cumulative privacy impact	<p data-bbox="336 479 1091 510"><i>Cumulative privacy impact and ethics of administrative data use</i></p> <p data-bbox="336 544 1374 730">Advances in technology have removed many of the practical barriers that previously limited collection, storage and processing of data on a massive scale. Removal of those barriers has created enormous opportunities from a statistics and research standpoint. However, it also creates privacy risk, including incremental and cumulative privacy risk over time.</p> <p data-bbox="336 763 1398 1234">One stakeholder consulted for the PIA stated that: ‘[i]n democratic societies such as ours, privacy’s chief function is in managing social boundaries, whether it be boundaries between people, between individuals and private business or between individuals and the government. These boundaries are essential for guarding against the actual or perceived misuse of power and for creating the conditions for all of us to develop autonomously as human beings.’ That stakeholder further noted, ‘The fact that the data may not be personally identifying or may not be used to “watch what people are doing”, does not mean that the collection of information is not a privacy issue. Surveillance is problematic because it violates social boundaries. Without adequate safeguards, this violation can be harmful to individuals, the government, and broader society.’ In that stakeholder’s view, the ABS’s proposed use of administrative data constituted a form of surveillance, the impact of which was compounded by lack of individual consent.</p> <p data-bbox="336 1267 1374 1417">The 2020 PIA on administrative data recommended that the ABS take steps to manage cumulative privacy risk. The ABS response stated that it was considering establishing a data ethics advisory committee to advise the Australian Statistician on ethical considerations concerning innovative ABS data use initiatives.</p> <p data-bbox="336 1451 1406 1832">IIS understands that ABS has considered options for data ethics assessments and is not proceeding with establishing a data ethics advisory committee at this time. The ABS has a structured approach to expansion of use of administrative data and expects to develop a data ethics framework to guide data uses. The framework will be based on the forthcoming Data Ethics Framework for the Australian Public Service (APS) and application of the principles of integrity respect and transparency. While the ABS has some mechanisms offering broad oversight and direction on data ethics issues, a more formal data ethics framework would be useful, especially considering the expansion of proposed administrative data use for 2026. Therefore, we are recommending a more structured approach to data ethics considerations regarding administrative data use.</p> <p data-bbox="336 1865 647 1888">See Recommendation 8.</p>

9.5 Summary and recommendations

Consideration of proportionality (use case 1)

The ABS's proposed collection and use of administrative data in connection with use case 1 is a significant expansion of its activities in this area and necessarily carries with it privacy risk. Notwithstanding the many protections the ABS will put in place to protect the data (including processing it largely in un-identified form and applying data separation principles), IIS considers this an area of activity requiring caution and transparency. Collection of population-wide (but limited detail) electricity usage data, in particular, represents a potentially significant insight into the private lives of Australians.

During the Phase 1 PIA, IIS recommended that the ABS formally consider whether the proposed use of administrative data to determine Census night occupancy and the intrusion on individual privacy was justified and proportionate to the anticipated benefits. The ABS accepted this recommendation. We suggest the ABS prioritise addressing that recommendation before progressing further with use case 1.

Restriction of use and retention (use case 1)

Noting the privacy sensitivities and impact of use case 1 (outlined above and in the APP analysis), IIS has opted to formally recommend the ABS limit use of the administrative data in question to the purpose of determining Census-night occupancy, and the related secondary purpose of testing occupancy models for the following Census. We note that the ABS is still considering how it will bring this administrative data into the agency – whether just for the Census or under a wider multi-use agreement. In the case of a multi-use agreement, other uses and activities involving the data may be permitted – those other uses and activities are outside the scope of this PIA, though the ABS advised IIS that a multi-use agreement would be subject to its usual privacy governance processes including a PTA and possible PIA.

We also recommend removal of administrative data from Census systems five years after Census night 2026. On this latter point, one stakeholder commenting on an earlier version of this recommendation during the drafting process expressed the view that 'permanently de-identifying' the data would be inadequate, and that complete destruction would be better to remove the risk of re-identification. We agree though note that final disposal of this data will be subject to any wider multi-use agreements in place.

While these recommendations are foundationally concerned with best practice, IIS notes that the amount of data to be collected and processed along with possible sensitivities in the community about the particular data to be used, indicate that clear use limitation may reassure the community.

These recommendations apply to administrative data used for Census night occupancy determinations. They do not apply to data already held by the ABS (such as PLIDA data) which are enduring data assets. It also does not apply to the ABS's administrative data use outside of the 2026 Census (which would be subject to the ABS's usual privacy governance and assessment processes).

Awareness of ABS use of administrative data in the Census (use cases 1 and 2)

In our APP analysis above, it became clear that, to meet ‘fairness’ and ‘notice’ requirements in the Privacy Act, the ABS needs to do more to ensure individuals are aware of this collection and use of administrative data about them. During the Phase 1 PIA, IIS recommended the ABS develop communication material to explain administrative data use. In the course of this Phase 2 PIA, the ABS drew our attention to the many channels through which the ABS makes information available to the public including via: [media releases](#), [media backgrounders](#), [collection notices](#), [privacy statements](#), publication of [PIAs](#) including responses, [social media engagement](#), [web content](#) relating to Census and [data integration](#) activities.

The ABS’s transparency on its data handling activities is commendable. We acknowledge the significant effort the ABS makes to make the public aware of how it collects and uses personal information. These communication channels are important. The privacy analysis and consultation conducted during this Phase only emphasised how important communicating with the public is to explain what administrative data is being collected and how it is being used. The Phase 1 PIA recommended that the ABS develop communications material leading up to the 2026 Census that explains to the public:

- What the ABS is proposing to do and its benefits
- The kinds of administrative data involved, how it will be collected and how it will be handled
- The safeguards in place to prevent secondary uses and disclosures of the administrative data
- The impact of the proposal on individuals’ privacy, and how this will be managed by the ABS.

In line with this Phase 1 recommendation, IIS also recommends testing the effectiveness of communications material in raising public understanding. This recommendation also goes to compliance with the ‘fairness’ limb of APP 3.5 (see analysis above).

Strengthening data ethics consideration of administrative data use (use cases 1 and 2)

During consultation on the draft PIA recommendations, IIS received only limited feedback from stakeholders though did receive strong support from one stakeholder for the recommendation concerning data ethics (**Recommendation 8**). Another stakeholder expressed the view that ‘data ethics’ may not be the appropriate term in this case and that good data governance or responsible data practices might better capture the intentions of the recommendation.

IIS acknowledges that data governance and responsible data practices are important. However, in this case, IIS wishes to align this recommendation with the concept of data ethics as understood in the wider statistics community.¹⁰ In particular, **Recommendation 8** is concerned with ensuring the ABS marshals its existing ethics arrangements in a methodical, repeatable way with regard to administrative data use. In other words, the ABS should follow a structured approach to consideration of data ethics for projects in which new or novel ethics issues may arise.

¹⁰ See for example, papers on data ethics from the [2024 Conference of European Statisticians](#). See also data ethics arrangements in statistics offices in other jurisdictions such as the [United Kingdom](#) and [Canada](#).

In meeting this recommendation, it is open to the ABS to use the forthcoming APS-wide Data Ethics Framework as a basis for ethics consideration of administrative data use.

Recommendation 4 – Include information about administrative data collection and use in the Census 2026 Privacy Statement

Compliance recommendation

Include information about administrative data collection and use in the Census 2026 Privacy Statement including information about the specific types of administrative data to be collected and used. In implementing this recommendation, give regard to APPs 3.5 (Fairness) and 5 (Notice).

Recommendation 5 – Test the effectiveness of awareness raising activities in relation to administrative data use in the Census

Best practice recommendation

Test the effectiveness of communications and awareness raising activities relating to administrative data use in the lead up to the Census. Do this by gathering evidence about levels of understanding in the wider community about ABS administrative data use and the effectiveness of communications activities. If the results indicate low understanding, develop a communications strategy to improve understanding on this matter in the wider community.

Recommendation 6 – Restrict use of non-PLIDA administrative data collected for determining Census night occupancy

Best practice recommendation

Restrict use of (non-PLIDA) administrative data collected for determining 2026 Census night occupancy to this purpose and the related secondary purpose of enabling development and testing of occupancy models for the following Census. Or, if the administrative data has been acquired by the ABS under a wider data sharing agreement, ensure use of the data in connection with the Census (that is, the scope of activities covered by this three-phase PIA) is limited to the purpose of determining 2026 Census night occupancy and the related secondary purpose of enabling development and testing of occupancy models for the following Census in 2031.

Given certain heightened privacy risks associated with the ABS's collection and use of the proposed administrative datasets (outlined in the analysis accompanying this recommendation), this recommendation aims to assure the community that use of the data will be strictly limited.

Recommendation 7 – Remove administrative data used for determining Census night occupancy from Census systems five years after Census 2026

Best practice recommendation

Remove records of administrative data (used for determining Census night occupancy) from Census systems (that is, systems used to support data processing associated with use case 1) five years after Census 2026. Given certain heightened privacy risks associated with the ABS's collection and use of the proposed administrative datasets (outlined in the analysis accompanying this recommendation), this recommendation aims to assure the community that use of the data will be strictly limited.

Recommendation 8 – Take a structured approach to data ethics oversight of proposed administrative data uses in the 2026 Census

Best practice recommendation

Ensure the approach to data ethics is well-structured by formalising the process for assessment and oversight of data ethics considerations relating to proposed administrative data use cases in the Census. This means:

- Having a formal structure of internal accountability for decision-making where data ethics questions or implications may arise (i.e., decisions about how and to what extent administrative data will be used in the Census), which ensures visibility and accountability to senior management, and
- Using this formal structure to consider:
 - Data ethics implications of each proposed administrative data use case
 - Questions of proportionality to the problem being solved, real or perceived agency overreach, and
 - The cumulative impact of successive expansions to administrative data use, and
- Reporting publicly on the outcome of internal data ethics processes to foster trust and transparency.

In meeting this recommendation, it is open to the ABS to implement the forthcoming APS-wide Data Ethics Framework and use this as the basis for ethics consideration (if applicable and available).

10. Business Locations Asset

The ABS is currently developing a Business Locations Asset (BLA) in the form of a register of ABNs and business location variables which aims to include national coverage of business operating locations.

The purpose of the BLA is to support the Australian Climate Service and its objectives of enhancing disaster risk and resilience intelligence by providing precise information on where businesses operate, which is essential for assessing regional economic exposure and vulnerability. It also aids in the development of regional economic indicators within the National Assessment Series and supports projects for the National Climate Risk Assessment.

10.1 Changes expected in 2026

In relation to the development of the BLA, the ABS is anticipating the following changes for the 2026 Census:

- *Use of Census data to enhance the BLA* – the ABS is exploring the possibility of using 2026 Census data to provide a fuller picture of business operating locations (going beyond registered business addresses which is often limited to the head office location as represented on the ABS Business Register).

10.2 Personal and other information involved

The information involved includes:

- Statistical information (Census) – collected via Census forms, including the respondent's employer's business name, respondent's employer's industry and respondent's workplace address.

IIS understands that the BLA will contain business addresses from sources other than the Census (for example, the business address registered with an ABN) and that Census data would be used to enhance that business address information. As noted above, this would ensure a more accurate picture of business operating locations across Australia beyond head office addresses.

In relation to Census data, the ABS advised that it would only include addresses of incorporated businesses (unincorporated businesses would be excluded). Further, any business addresses matching either the 'front of form address' (i.e. the address the respondent is at on Census Night), or a respondent's current residential address or past residential address are also excluded from inclusion in the BLA. This exclusion is regardless of whether the business is incorporated or unincorporated.

In effect, this means that residential addresses will be excluded from the BLA (other than cases of a multi-use building complex containing both business and residential addresses; however, the business address would be distinguished by the unit, flat, apartment or shop number).

10.3 Stakeholder feedback

Consultation with stakeholders revealed that while most were not opposed in general to the establishment of the BLA, several raised concerns about potential collection of residential addresses (for example, in the context of a sole trader or a person who predominantly works from home). It was noted that individuals may have reservations about their address information being used for this secondary purpose. The ABS has since clarified that workplaces located at the residential address of the respondent would be excluded from inclusion in the BLA.

10.4 APP analysis and other privacy risks

Analysing the privacy impact of this proposed use of Census data raises two core issues – first, whether the data in question is personal information for the purposes of the Privacy Act, and second, if so, whether the proposed use meets the requirements of the APPs. IIS found that the initial data processing is likely to involve personal information but that, once processed for inclusion in the BLA, the information is unlikely to qualify as personal information. Therefore, the main privacy compliance consideration is the secondary use of Census data for that processing to prepare the data for inclusion in the BLA. Key APPs applying in this case include APPs 5 (Notice) and 6 (Use).

APP	Comments and analysis
Definition of PI	<p><i>Data from Census processed for inclusion in the BLA</i></p> <p>The ABS intends to use Census data including the respondent’s employer’s business name, respondent’s employer’s industry and respondent’s workplace address. In addition, in order to exclude residential addresses, the ABS would use the ‘front of form’ address and present and past residential addresses (inside form).</p> <p>IIS finds that, in combination, this information may meet the definition of personal information in the Privacy Act. However, once processed with residential and unincorporated business addresses removed, and with business names replaced with ABNs and addresses replaced with address IDs prior to inclusion in the BLA, IIS finds that this information is unlikely to meet the definition of personal information.</p>
APP 5	<p><i>Notice obligations in relation to use of Census data in the BLA</i></p> <p>Given the analysis in the row above, APP 5 will apply to the collection and use of the information to prepare it for inclusion in the BLA. APP 5 requires an agency to take reasonable steps to make an individual aware of certain matters when it collects personal information about the individual – this is commonly referred to as a privacy notice. APP 5.2 lists matters to be included in the notice. One of those matters (APP 5.2(d)) is the purposes for which the APP entity collects the information. Use of Census data to enhance the BLA would appear to be a new collection purpose that should be included in the Census Privacy Statement.</p> <p>With regard to the ABS’s 2021 Census Privacy Statement, BLA-related data processing would likely have been broadly covered by the statement that personal information is</p>

<i>APP</i>	<i>Comments and analysis</i>
	<p>collected for statistical activities including compilation, where compilation includes data integration and the ‘combining [of] data from two or more sources to create new and more valuable information.’ Other parts of the notice that may require update include the ‘Name and address collection’ section and the ‘Statistical projects involving names and addresses’ section.</p> <p>See Recommendation 9.</p>
APP 6	<p><i>Processing of Census data for use in the BLA</i></p> <p>IIS understands that, to prepare relevant Census data for inclusion in the BLA, the ABS will extract relevant variables, replace addresses with address IDs, replace business names with ABNs, remove unincorporated business ABNs and associated address IDs, and remove address IDs that match any residential address contained in the same Census form. The resulting dataset is unlikely to meet the definition of personal information. At that point the APPs, including APP 6, cease to apply.</p> <p>Though this data processing is a new use of Census data, IIS finds that it may fall within the primary purpose of collection: use for statistical purposes (including compilation and data integration) hence meeting APP 6.1 (which permits use of personal information for the primary purpose of collection). Or, if defined as a ‘secondary purpose,’ it is likely to meet the exception allowing a secondary use that is authorised by an Australian law (APP 6.2(b)) – in this case relevant provisions in the ABS Act and the Census and Statistics Act which authorise the ABS to collect, hold and use personal information for Census and statistics purposes.</p> <p>No further issues identified.</p>
<i>Other risks</i>	<i>Comments and analysis</i>
Public misunderstanding / loss of trust	<p><i>Transparency of Census data secondary uses</i></p> <p>Transparency of statistics and data integration activities fosters public trust, particularly in cases where personal information handling is otherwise not visible or obvious to the individual. As with its other statistics and data integration initiatives, the ABS should publish explanatory information on its website about the BLA and its purpose.</p> <p>See Recommendation 9.</p>
Function creep	<p><i>Future expansion of Census data for BLA-related purposes</i></p> <p>The current proposal for Census data use for the BLA is limited – with unincorporated business and business addresses matching a residential address of the respondent excluded. Future changes or expansions to the scope of BLA data processing beyond the 2026 Census are out of scope for this PIA. However, the ABS should be aware that any</p>

APP	Comments and analysis
	<p>such changes may trigger the application of additional APPs and should therefore be subject to its usual privacy governance checks and assessments.</p> <p>No further issues identified.</p>
Fit for purpose	<p><i>Testing approach in the 2025 ORE</i></p> <p>IIS understands that the ABS will test processes to extract and use Census data for the BLA during the 2025 ORE to support the development of a proof of concept for the Census main event. This offers an opportunity to check privacy arrangements are fit for purpose. For example, what was the rate of the incidence of residential addresses in the data after processing; were there unforeseen privacy risks identified during testing.</p> <p>See Recommendation 10.</p>

10.5 Summary and recommendations

The actual privacy impact of use of Census data to enhance the BLA appears to be low given the measures proposed to exclude residential addresses. For that reason, the main focus of the recommendations below is encouraging transparency regarding BLA-related processing of Census data. We also suggest more clarity on how the ABS explains its address disposal and retention practices generally. We note, for example, that the ABS plans to follow its policy of retaining Census address information for no longer than 36 months while administrative data containing address information and used in conjunction with the Census will be retained for longer. See **Recommendation 9**.

We also recommend testing the effectiveness of arrangements to protect privacy and exclude residential addresses in the 2025 ORE. See **Recommendation 10**.

Recommendation 9 – Clarify the ABS’s use and retention of address information (including use for BLA related processing) in the 2026 Census Privacy Statement.

Best practice recommendation

Clarify the ABS’s use and retention of address information in the 2026 Census Privacy Statement. In particular:

- Explain how address disposal no later than 36 months interacts with retention and use of address information in other projects and enduring datasets. (This should include explaining that addresses contained in administrative data used to support Census operations will be retained for longer.)
- Ensure the ‘Name and address collection’ section of the Statement (or 2026 equivalent section) and the ‘ABS statistical projects using names and addresses’ section of the Statement (or 2026

Recommendation 9 – Clarify the ABS’s use and retention of address information (including use for BLA related processing) in the 2026 Census Privacy Statement.

equivalent section) reflect any new uses or processing of address information (e.g. use for BLA-related processing).

- Publish explanatory information about the BLA which covers both the purpose of the BLA and the measures in place to safeguard privacy and process information securely. The Census 2026 Privacy Statement could link to this more detailed information.

Recommendation 10 – Test that BLA-related privacy arrangements are fit for purpose during 2025 ORE

Best practice recommendation

Use the 2025 ORE to identify possible unforeseen privacy risks concerning the use of Census data for inclusion in the BLA. Document identified privacy risks (if any) and proposed controls to enable review of BLA-related arrangements.

Appendix A. Glossary

Abbreviation or term	Expansion or definition
ABN	Australian Business Number
ABS	Australian Bureau of Statistics
ABS Act	<i>Australian Bureau of Statistics Act 1975 (Cth)</i>
Administrative data	Administrative data is information collected by government agencies, businesses or other organisations for various purposes, including registrations, transactions and record keeping, usually during the delivery of a service.
AI	Artificial Intelligence
ANZSCO	Australia and New Zealand Standard Classification of Occupations
APPs	Australian Privacy Principles
APS	Australian Public Service
ATO	Australian Tax Office
AWS	Amazon Web Services
BLA	Business Locations Asset
Census and Statistics Act	<i>Census and Statistics Act 1905 (Cth)</i>
CAT	Census Agent Tool
EMI	Enumeration Management System
HREC	Human Research Ethics Committee
IIS	IIS Partners (report author)
LLM	Large Language Model
MADIP	Multi-Agency Data Integration Project
MBUN	Meaningless but unique number

Abbreviation or term	Expansion or definition
ML	Machine Learning
OAIC	Office of the Australian Commissioner
ORE	Operational Readiness Exercise
PES	Post Enumeration Survey
PIA	Privacy Impact Assessment
PLIDA	Person Level Integrated Data Asset
PMO	Program Management Office
Privacy Act	<i>Privacy Act 1988 (Cth)</i>
PTA	Privacy Threshold Assessment
SADE	Scaled Analytical Data Environment
SRO	Senior Responsible Officer
WoAG	Whole of Australian Government

Appendix B. Documents reviewed and meetings held

B.1 Documents reviewed

Documents reviewed
1. Org Structure ABS
2. Census Data Protection Plan
3. Census - Strategic and Program Risks
4. Census High Level governance Plan
5. Census Privacy Plan
6. Census Privacy Strategy 2021 -2028
7. Census Contacts
8. Personal Information Mapping
9. Phase 2 Personal Information Questionnaire Address Register
10. Phase 2 Personal Information Questionnaire
11. Phase 2 Personal Information Questionnaire
12. Use of Administrative Data MADIP Data Flow
13. Phase 2 Personal Information Questionnaire
14. Personal Information Mapping
15. Phase 2 Personal Information Mapping
16. Phase 2 Personal Information Questionnaire
17. Coverage Flows
18. 2021 Digital Paper Services
19. Census Digital Service Refusals Process Mapping
20. Census Digital Service Contact Centre & Customer Support Process Mapping
21. Command Centre Strategic
22. Contact Centre and Customer Support

Documents reviewed
23. Digital and Papers Services Flow Mapping
24. Digital Service - Command Centre Strategic Flow Mapping
25. Phase 2 Personal Information Questionnaire
26. Refusals & Corro
27. Refusals and Ministerial
28. Data Integration Information Flows
29. Census Enumeration - EMI
30. Census Enumeration Model and procedures
31. Census Enumeration Inclusive Strategies
32. Census Enumeration Training Enumeration Integration
33. Phase 2 Personal Information Questionnaire
34. Phase 2 Personal Information Questionnaire
35. Phase 2 Personal Information Questionnaire
36. Phase 2 Personal Information Questionnaire
37. Flow Map - Post Enumeration
38. Phase 2 Personal Information Questionnaire
39. Census HR Procurement & Census Workforce Management
40. Census Workforce Management & Recruitment Payroll Training Field
41. Census WHS Data for SafeZone
42. Census Training
43. Census Inclusive Strategies
44. Aboriginal & Torres Strait Islander Strategies
45. Enabling Partners and Operational Development
46. Relationship Management and Strategy Development

Documents reviewed
47. 2021 Field Support Centre archived content.pdf
48. 2021 Work Health and Safety archived content.pdf
49. ABS Census 2026 PIA (Phase 2) - further follow-up actions 2024-05.docx
50. Census and WoAG Coding Capability _ 2 x PIAs_.pdf
51. Census Security Assurance Activities 2026 PIA.pdf
52. CONTAINS DIAGRAM - Draft Support plan V1.pdf
53. Field Knowledge archived content
54. ABS DataLab
55. Dwelling Level Electricity PTA - Final.pdf
56. Privacy Threshold Assessment - Census Synthetic Address Test Dataset FINAL.K
57. Privacy Threshold Assessment - Census Test Dataset.pdf
58. Privacy Threshold Assessment - Census Test
59. 2021 Census PIA_ABS response
60. 2022 Census PIA_Galexia
61. Kylie Russell Response re Operational Data
62. ADS survey findings
63. Customer Contact & Support
64. ACLD 2016.pdf
65. Information Flows NDDA ANDII.pdf
66. MADIP conceptual data flow.pdf
67. PLIDA Information flows
68. 18 Enabling Partners and operational development.pdf
69. 18 Relationship Management and Strategy Development.pdf
70. 20240124_Privacy Threshold Assessment - Safezone

Documents reviewed

71. Safe Zone Privacy Threshold Assessment.pdf

B.2 Meetings held with ABS teams

Meetings held	Date
Census Privacy / Data Protection	9-Apr-24
Census Privacy / Data Protection	15-Apr-24
Coverage & Data Quality	16-Apr-24
Logistics	16-Apr-24
Customer Experience	22-Apr-24
Data design	22-Apr-24
Address Team	23-Apr-24
TSD Census Enumeration	29-Apr-24
Digital Service	30-Apr-24
Census Dissemination	30-Apr-24
Location Information Team	30-Apr-24
Census Admin Data Ventures	30-Apr-24
Temporary Workforce #1	30-Apr-24
Data integration	1-May-24
Enumeration	2-May-24
Post Enumeration Survey	2-May-24
Temporary Workforce #2	13-May-24
Enumeration #2	3-Jun-24

Meetings held	Date
Census Admin Data Ventures #2	4-Jun-24
Enhanced Coding Capability	22-Jul-24
myGov	5-Aug-24

Appendix C. List of external consultation stakeholders

C.1 Roundtable participants

Individuals
1. Dr Ian Oppermann, former NSW Government Chief Data Scientist, Co-Founder, ServiceGen
2. Edward Santow, Director, Policy & Governance, UTS Human Technology Institute
3. Katharine Kemp, Associate Professor, Faculty of Law & Justice, UNSW
4. Kimberlee Weatherall, Professor of Law, University of Sydney, Chief Investigator, ARC Centre of Excellence for Automated Decision-Making and Society
Organisations
1. The Ethics Centre
2. Relational Insights Data Lab, Griffith University
3. NSW Information and Privacy Commission
4. NSW Council for Civil Liberties
5. Australian Government Department of Education
6. Australian Government Department of Employment and Workplace Relations

C.2 One-on-one meetings

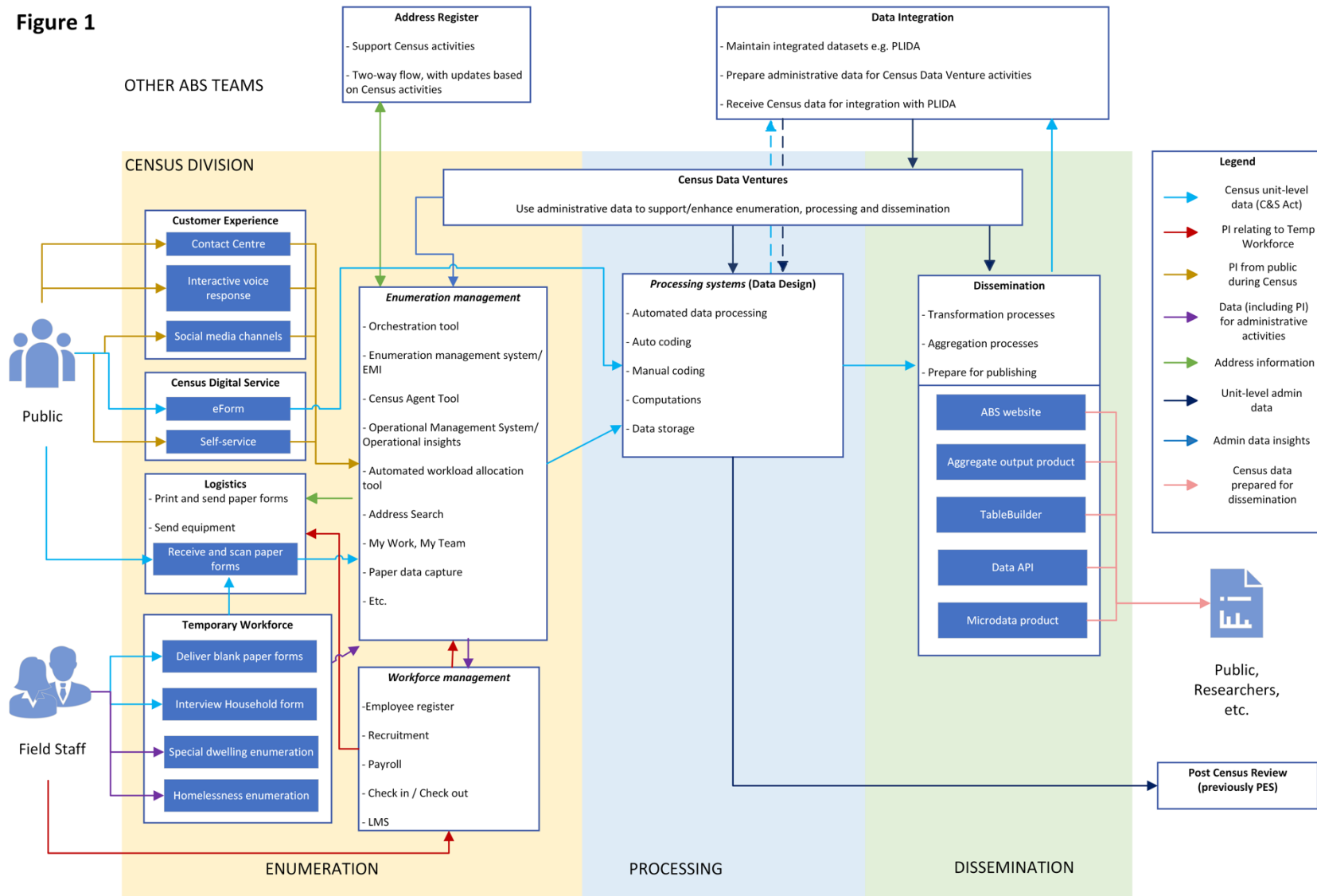
Individual/Organisation
7. Lyria Bennett Moses, Associate Dean, Faculty of Law and Justice, University of New South Wales
8. Queensland Council for Civil Liberties

C.3 Written submissions

Individual/Organisation
9. The Office of the Victorian Information Commissioner

Appendix D. Overview of personal information flows

Figure 1





INFORMATION INTEGRITY SOLUTIONS PTY LTD

PO Box 978, Strawberry Hills NSW 2012, Australia

P: +61 2 8303 2438

E: contact@iispartners.com

www.iispartners.com

ABN 78 107 611 898

ACN 107 611 898



IIS Partners
INFORMATION INTEGRITY SOLUTIONS