galexia

Australian Bureau of Statistics

Australian Bureau of Statistics (ABS)

2021 Census Privacy Impact Assessment (PIA)

(GC590 | ABS2019.286)

April 2020 (FINAL)

Contact: Galexia
Level 11, 175 Pitt St, Sydney NSW 2000
Ph: +61 2 9660 1111
www.galexia.com
Email: manage@galexia.com

Document Control

Client

This document has been written for the Australian Bureau of Statistics (ABS).

Document Purpose

This document is the PIA for provision of an independent public Privacy Impact Assessment (PIA) for the 2021 Census.

Document Identification

Document title	ABS – 2021 Census Independent PIA – PIA
Document filename	gc590_abs_2021_census_pia_PIA_20200430_FINAL.pdf

Client Details

Client	**Australian Bureau of Statistics (ABS)** <www.abs.gov.au> ABS House45 Benjamin Way Belconnen ACT 2617
Client Reference	ABS2019.286

Consultant Details

Galexia Contact	**Peter van Dijk** (Managing Director) Galexia <www.galexia.com> Level 11, 175 Pitt St, Sydney NSW 2000, Australia p: +612 9660 1111 m: +61 419 351 374 e: manage@galexia.com
Galexia Reference	GC590
Project Email	abscensus@galexia.com

Contents

1. Overview and Scope

Galexia has been commissioned by the Australian Bureau of Statistics (ABS) to prepare an independent Privacy Impact Assessment (PIA) for the 2021 Census.

The core of this PIA concentrates on consumer data.

Consumer data, for the purposes of this PIA means data such as:

- Statistical data provided by consumers when completing the Census form;
- General consumer data regarding individuals who communicate with the ABS Contact Centre; and
- Administrative data relating to households.

Employee data is also **briefly** covered as an adjunct to this PIA and appears solely as an Appendix (Refer to Appendix E – Employee Data).

Employee data, for the purposes of this PIA means data such as:

- Data relating to ABS employees engaged in Census activities; and
- Data relating to ABS contractors engaged in Census activities.

1.1. Audience and Currency

This version of the PIA is current as at 30 April 2020 and is intended for public release and response from ABS.

1.2. Approach

The PIA was conducted in accordance with *PIA Guidelines*[1] issued by the Office of the Australian Information Commissioner (OAIC). The ABS has agreed to respond to and publish the PIA as part of their ongoing consultation with stakeholders and the community.

This PIA considers alignment with privacy and ABS legislation, user acceptance and public perception issues. This PIA makes a broad range of recommendations for mitigating privacy risks, including changes to the design and implementation of Census processes, practical privacy compliance steps and enhanced privacy governance arrangements.

Galexia's advice in this PIA concentrates on the following areas:

- **Structural Privacy Recommendations**
  This PIA includes major Structural Privacy Recommendations – key mechanisms to ensure a lasting, layered and sustainable Privacy-by-Design / Privacy-in-Depth approach is adopted for the Census (for 2021 and beyond);
- **Australian Privacy Principles (APPs)**
  This PIA assesses the proposed 2021 Census program against the Australian Privacy Principles (APPs) in the *Privacy Act 1988*;
- **ABS Legislation Compliance**
  This PIA assesses the proposed 2021 Census program against the privacy and security requirements contained in the ABS's own legislation;
- **Australian Government Agencies Privacy Code Compliance**
  This PIA assesses the proposed 2021 Census program against the Australian Government Agencies Privacy Code;

[1] Office of the Australian Information Commissioner, Australian Government, *Guide to undertaking privacy impact assessments* (May 2014) <www.oaic.gov.au/privacy/guidance-and-advice/guide-to-undertaking-privacy-impact-assessments>.

- **Additional Governance Requirements**
  This PIA briefly assesses the proposed 2021 Census program against general governance requirements, for example best practice guidance, lessons from other similar schemes, etc.;
- **Social Licence**
  This PIA briefly identifies several measures that can be taken to assist with the development of a Social Licence for the Census;
- **Galexia Privacy Risk Identification**
  This PIA includes a summary privacy risk assessment, following earlier work on risk during the PIA process; and
- **Employee Data**
  An Appendix briefly covers data relating to ABS employees and contractors.

The information contained in this PIA is based on:

- Numerous meetings with ABS staff, including senior management, technical staff, policy and legislation staff, field operations staff and the data linkage centre team (more than 30 ABS stakeholder meetings and more than 26 project team and senior management meetings) – Refer to Appendix D – Stakeholders and Meetings;
- Meetings with 12 key external stakeholders – Refer to Appendix D – Stakeholders and Meetings;
- Examination of documentation related to previous Census operations and planning for the proposed 2021 Census program (more than 100 documents and diagrams);
- Review of relevant privacy legislation, ABS legislation and guidelines;
- Consideration of reviews and commentary of earlier Censuses; and
- ABS feedback on earlier tasks in the PIA process.

1.3. Scope

The scope of the overall PIA is limited to the following items:

In Scope	Out of Scope
• High level identification of potential compliance issues in the context of the Commonwealth privacy legal framework	• Compliance with specific sectoral legislation or state and territory legislation
• Review of a moderate number of *key* documents	• Review of the entire suite of ABS Census documentation
• Regular internal stakeholder consultation • A reasonable amount of external consultation	• Broader community engagement, such as a call for public submissions.
• Very high level identification and review of legal documentation	• Detailed legal advice
• Consideration of security issues relevant to privacy compliance	• Comprehensive security assessment or testing
• Review any relevant research into likely community opinion	• Detailed original study or assessment of public attitudes
• Assess the overall privacy impact of the Census questions as already proposed by the ABS	• Provide input into the selection of new Census questions (this process was completed prior to the commencement of the PIA)

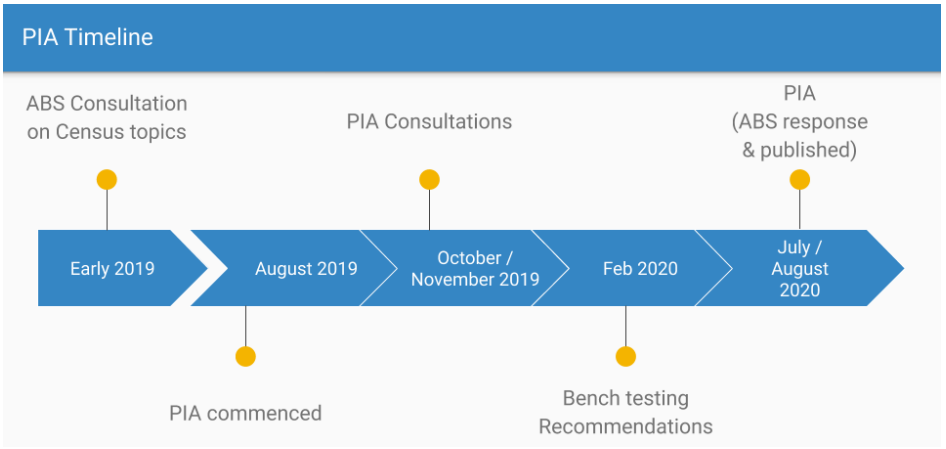
1.4. Methodology

In the development of this PIA, a collaborative approach with the ABS and identified external stakeholders was undertaken.

The methodology taken by Galexia involved:

- Undertaking an extensive information review of documents and information on the Census process including privacy policies and record keeping policies;
- Undertaking a mapping of key personal information flows;
- Assessing compliance with relevant legislation, guidelines and standards from privacy regulators and government agencies, community expectations and attitudes, etc.;
- Identifying privacy impacts and risk areas including examining how the ABS handles consumer data, the potential impact on the community, security impacts, and how the Census meets community expectations;
- Internal and external stakeholder consultation – the stakeholder consultation process was directed at privacy and civil society advocates, key university academics and regulators;
- Providing an Initial Issues Guidance with candidate findings and suggested next steps to the ABS – as part of Galexia's 'no surprises' approach (this resulted in some early advice being implemented by the ABS, and this is noted in the text of the PIA. For example APP 1. Privacy policy issues resolved);
- Undertaking a second round of stakeholder consultations to bench test the candidate findings; and
- Developing a final set of recommendations based on the candidate findings and feedback received.

The overall timing of the PIA process is summarised in the following timeline:



1.5. Internal and External Stakeholders

Galexia conducted extensive internal consultations (with unlimited access to ABS teams and senior executives) and a targeted external stakeholder consultation during the development of the PIA.

The initial engagement was on internal stakeholder consultations and key external stakeholders – privacy, consumer advocacy and civil society organisations, university academics and privacy regulators.

A stakeholder consultation strategy was developed and agreed with the ABS.

A second round of stakeholder engagement was undertaken to benchmark candidate findings.

Refer to Appendix D – Stakeholders and Meetings.

2. Executive Summary – High Level Privacy Findings and Recommendations

2.1. Overview

This PIA presents:

- **Three Major Structural Recommendations** – Galexia is proposing key mechanisms to ensure a lasting, layered and sustainable Privacy-by-Design / Privacy-in-Depth approach is adopted for the Census; and
- **17 Detailed Recommendations** – focussing on risk management and compliance with relevant legislation, codes and guidelines for the 2021 Census.

2.2. Privacy Status Dashboard for the 2021 Census PIA

The following table summarises Galexia's privacy compliance and status assessment of the 2021 Census as at April 2020:

Australian Privacy Principles (APPs) (Sections 6-19)	**Action / Status**
Classification of Data – Is the Data 'personal information' or 'sensitive information'?	n/a
APP 1 – Openness and Transparent Management of Personal information	**Action required**
APP 2 – Anonymity and Pseudonymity	**Compliant**
APP 3 – Collection of Solicited Personal Information	**Compliant (Further measures possible)**
APP 4 – Dealing with unsolicited personal information	**Compliant**
APP 5 – Notification of the Collection of Personal Information	**Action required**
APP 6 – Use or disclosure of Personal Information	**Compliant**
APP 7 – Direct Marketing	**Compliant**
APP 8 – Cross-border Disclosure	**Compliant**
APP 9 – Government Related Identifiers	**Compliant**
APP 10 – Quality of Personal Information	**Compliant**
APP 11 – Security (Independent Security Risk Assessments)	**In progress**
APP 11 – Security (Data Retention – Names)	**Action required**
APP 11 – Security (Data Retention – Addresses)	**Action required**
APP 12 – Access (General access rules)	**Action required**
APP 12 – Access (Time Capsule access rules)	**Action required**
APP 13 – Correction	**Compliant**
ABS Legislation (Section 20)	**Action / Status**
Census and Statistics Act 1905 (Cth)	**Compliant**
Australian Bureau of Statistics Act 1975 (Cth)	**Compliant**
APS Privacy Code Requirements (Section 21)	**Action / Status**
A. Privacy Management Plan	**Compliant**
B. Privacy officer	**Compliant**
C. Privacy champion	**Compliant**
D. PIAs	**In progress**
E. PIA register	**Compliant**

F. Privacy training	**Compliant**
G. Monitoring and review	**Compliant**
Additional Governance Requirements (Section 22)	**Action / Status**
A. Explaining the legal basis for data linkage	**Compliant (Further measures possible)**
B. Managing agreements with third parties and contractors	**In progress**
C. Managing Function Creep (Legislative basis for use of data)	**Action Required**
D. Managing Function Creep (Application of the proposed DATA Framework)	**Action Required**
E. Managing Function Creep (Application of the proposed DATA Framework to the Time Capsule)	**Action Required**
F. Managing Function Creep (Inclusion of health information in the Time Capsule)	**Action Required**
G. Reviewing the consequences for not responding to a Notice of Direction	**Action Required**
Social Licence Requirements (Section 23)	**Action / Status**
A. A sound basis for believing in the integrity and accountability of the ABS	**Action required**
B. Consumers feel they have some control over how their own data is used and by whom	**Action Required**
C. Consumers have the ability to choose to experience some of the benefits of data use themselves	**Compliant**
D. Consumers understand the potential community-wide benefits of data use	**Compliant**

2.3. Recommendation Summary

Component / APP	Galexia Recommendation
Structural Recommendation 1: Census Privacy Strategy – The ABS should develop and implement a 7-8 year Census Privacy Strategy that covers more than one Census.	
Structural Recommendation 2: Principles based approach to name encoding for data linkage – The ABS should develop and implement a principles based approach to the issue of name encoding for data linkage.	
Structural Recommendation 3: Principles based approach to managing re-identification risk – The ABS should develop and implement a principles based approach to managing re-identification risk.	
APP 1 – Openness and Transparent Management of Personal Information	**Recommendation 1: Develop and maintain separate Census Privacy Policy sections.** Each Census Privacy Policy sub-section or appendix should be clearly dated and an archive of prior policies should be maintained (for the 2016 and 2021 Censuses at least).
APP 3 – Collection of Solicited Personal Information	**Recommendation 2: Promote alternatives to third party collection.** The ABS should explore measures to address the extent of third party collection of data. For example, more could be done to promote the option to use individual paper and online forms.
APP 5 – Notification of the Collection of Personal Information	**Recommendation 3: Clarify privacy notice information on the potential consequences for not providing information.** The ABS should develop a clear and consistent set of wording to inform consumers about the consequences of not completing the Census.
APP 11 – Security (Independent Security Risk Assessments)	**Recommendation 4: Conduct independent security risk assessments for key 2021 Census components.** The ABS should commission independent security risk assessments for key components of the 2021 Census: • An 'end to end' assessment (this has been commissioned); • A specific assessment of the cloud platform (this may be covered by existing security certifications); and • The Time Capsule (this has yet to be commissioned).

APP 11 – Security (Data Retention – Names)	Recommendation 5: **Shorten data retention periods for names.** The ABS should review and significantly reduce the data retention periods for names. If the reduction needs to be staggered to meet business needs, this should be reduced over the next two Censuses. As a minimum the data retention period for names should be re-set as 18 months for the 2021 Census.
APP 11 – Security (Data Retention – Addresses)	Recommendation 6: **Shorten data retention periods for addresses.** The ABS should review and, if possible, reduce the data retention periods for addresses. If the reduction needs to be staggered to meet business needs, this should be reduced over the next two Censuses. As a minimum the data retention period for addresses should be reduced for the 2021 Census to a period of 24-36 months.
APP 12 – Access (General access rules)	Recommendation 7: **Clarify access rules for different categories of data.** The ABS should clarify the access rules that apply to each category of data, and set these out clearly in the ABS Privacy Policy, including: • Core Census data (i.e. statistical data); • ACLD; • Integrated Census data (e.g. MADIP); • Time Capsule; and • Other non-statistical data (e.g. Contact Centre records).
APP 12 – Access (Time Capsule access rules)	Recommendation 8: **Clarify and strengthen access restrictions to data held in the Time Capsule.** The ABS should clarify and strengthen access rules that apply to data held in the Time Capsule, noting examples of international pressure for early access to similar data.
Australian Government Agencies Privacy Code (PIAs)	Recommendation 9: **Conduct additional independent PIAs for activities that are 'renewed' for each Census**. The ABS should consider conducting additional independent PIAs for the ACLD and the Time Capsule.
Additional Governance Requirements (A. Explaining the legal basis for data linkage)	Recommendation 10: **Clarify the prohibition on using multiple Census collections in MADIP.** The ABS should clarify and highlight the prohibition on using multiple Census collections for longitudinal study via MADIP.
Additional Governance Requirements (B. Managing agreements with third parties and contractors)	Recommendation 11: **Establish and maintain a register of third party agreements.** The ABS should establish a register of third party agreements and use this to drive / promote a consistently high level of privacy protections and privacy management.
Additional Governance Requirements (C. Managing Function Creep – Legislative basis for use of data)	Recommendation 12: **Clarify ABS legislation to set out permitted and precluded purposes for use of Census data.** The ABS should explore ways to clarify legal restrictions on the use of Census data. Options might include a guideline, declaration or a potential legislative amendment.
Additional Governance Requirements (D. Managing Function Creep – Application of the DATA Framework)	Recommendation 13: **Clarify the relationship between Census data and the proposed Data Availability and Transparency Act (DATA) Framework.** The ABS should consider whether or not to exclude Census data from the proposed DATA Framework, and the potential impact of the DATA Framework on both the generic secrecy provisions that apply to ABS data and the specific privacy protections that apply to Census data.
Additional Governance Requirements (E. Managing Function Creep – Application of the DATA Framework to the Time Capsule)	Recommendation 14: **Seek an exemption from the proposed DATA Framework for the Time Capsule.** The ABS should seek an exemption for the Time Capsule from the proposed Data Availability and Transparency Act (DATA) Framework. This recommendation should be seen as the minimum ABS response to the proposed DATA Framework, and not the full response.

Additional Governance Requirements (F. Managing Function Creep – Inclusion of health information in the Time Capsule)	Recommendation 15: **Remove the new health data collected in the 2021 Census from data submitted to the Time Capsule.** The ABS should ensure that responses to the new long-term health conditions question are not included in the Time Capsule, and that this is clearly explained to consumers.
Additional Governance Requirements (G. Reviewing the consequences for not responding to a Notice of Direction)	Recommendation 16: **Review the consequences for refusing to complete the Census.** The ABS should reform the refusals and prosecution process to implement a better balance between response rates and consequences for individuals facing prosecution.
Employee Data (APP 11 – Security)	Recommendation 17: **Conduct an independent security review for the MyWork App**. The ABS should commission an independent security risk assessment for the proposed MyWork App.

2.4. Structural Privacy Recommendations

This PIA presents three major Structural Recommendations. These are key mechanisms to ensure a lasting, layered and sustainable Privacy-by-Design / Privacy-in-Depth approach is adopted for the Census (for 2021 and beyond).

Structural Recommendation 1: Census Privacy Strategy – The ABS should develop and implement a 7-8 year Census Privacy Strategy that covers more than one Census.

During the PIA process and stakeholder consultations it emerged that some privacy issues and concerns related to the Census may be exacerbated by the 'one-off' approach to Census privacy management.

In developing this recommendation, Galexia suggests that the Census Privacy Strategy should cover a period of 7-8 years, so that it straddles two Census periods.

The contents of the Census Privacy Strategy should include:

- Integration of multiple PIAs;
- Integration of the PIA with the development of Census content;
- Integration of key stakeholder consultation on Census privacy issues; and
- Inclusion of long-term privacy objectives and targets.

More detail of the approach is outlined at: Section 5 – Structural Recommendation 1: Census Privacy Strategy.

Structural Recommendation 2: Principles based approach to name encoding for data linkage – The ABS should develop and implement a principles based approach to the issue of name encoding for data linkage.

Name encoding is one of the key processes used by the ABS to link Census data with other datasets. During the PIA process it became apparent that this process is the subject of considerable concern amongst external stakeholders, and that the process is poorly understood outside the ABS.

This PIA sets out a principles based approach to managing this issue, which could be used by the ABS on an ongoing basis. This approach would give confidence to stakeholders that the issue was the subject of regular review and oversight.

More detail of the approach is outlined at: Section 5 – Structural Recommendation 2: Principles based approach to name encoding for data linkage.

Structural Recommendation 3: Principles based approach to managing re-identification risk – The ABS should develop and implement a principles based approach to managing re-identification risk.

During the PIA process it became apparent that re-identification risk is the subject of considerable concern amongst external stakeholders.

This PIA sets out a principles based approach to managing this issue, which can be used by the ABS on an ongoing basis. This approach would give confidence to stakeholders that the issue was the subject of regular review and oversight.

Although the ABS has been following this approach for some time, it would benefit from improved documentation, a more formal approach to engaging with stakeholders, and enhanced oversight and review.

More detail of the approach is outlined at: Section 5 – Structural Recommendation 3: Principles based approach to managing re-identification risk.

2.5. Australian Privacy Principles (APPs)

This PIA is written in the light of current Commonwealth privacy legislation – the *Privacy Act 1988 (Cth)*. The Act sets out the Australian Privacy Principles (APPs),[2] which regulate the collection, use and disclosure of personal information by Commonwealth Agencies and private sector organisations.

This PIA assesses the proposed 2021 Census arrangements against the APPs.

The following table summarises the main findings and recommendations with links to further information and detailed discussion (Sections 6 to 19) in the text:

Australian Privacy Principle (APP)	Action / Status	Galexia Commentary	Galexia Recommendation
Classification of Data – Is the Data 'personal information' or 'sensitive information'?	n/a	The 2021 Census will incorporate questions requiring a mix of personal information and sensitive personal information. The presence of sensitive information has implications for APP 3 and APP 6 (discussed below). It also raises the overall security profile of the proposal (discussed in APP 11 below).	–
APP 1 – Openness and Transparent management of personal information	**Action required**	The ABS is drafting a new overarching privacy policy to cover all of its activities. During the development of this PIA, Galexia has provided input on key issues that have now been addressed in the new draft privacy policy (Refer to APP 1. Privacy policy issues resolved). One outstanding issue is the question of whether there should be a stand-alone Census Privacy Policy. This PIA recommends that the privacy policy (whether it is a generic ABS Privacy Policy or a stand-alone Census Privacy Policy) should have a clear, separate section covering the specific features of each Census. This is because the content and the data retention periods change for each Census.	**Recommendation 1: Develop and maintain separate Census Privacy Policy sections** Each Census Privacy Policy sub-section or appendix should be clearly dated and an archive of prior policies should be maintained (for the 2016 and 2021 Censuses at least).
APP 2 – Anonymity and Pseudonymity	**Compliant**	The ABS provides anonymity to users in appropriate circumstances – for example general web site visitors can access information about the Census without providing personal information. All other data collected via the 2021 Census is covered by exceptions to the anonymity principle. For example, the ABS is authorised to collect names on Census forms so that they can reconcile records where an individual appears on more than one form (e.g. an individual form and a household form completed by a third party).	–

[2] The 13 APPs are in Schedule 1 of the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* <www.legislation.gov.au/Details/C2015C00053>, which amended the *Privacy Act 1988* (Cth) <www.legislation.gov.au/Details/C2020C00025>. They came into force on 12 March 2014.

APP 3 – Collection of solicited personal information	**Compliant** **Further measures possible**	This PIA is being completed after the finalisation of the Census topics and questions, so consideration of the content of the Census questions is limited. Some concerns regarding the Census questions are addressed in Structural Recommendation 1: Census Privacy Strategy. APP 3 requires entities to only collect information that is reasonably necessary. The ABS does apply a data minimisation approach to the collection and use of personal information in both the original collection process and in ABS data integration programs. APP 3 requires entities to limit the collection of data from third parties. A significant amount of data is collected from third parties in the Census. Although this is done in compliance with ABS legislation and the *Privacy Act,* more could be done to encourage the use of individual forms.	Recommendation 2: **Promote alternatives to third party collection** The ABS should explore measures to address the extent of third party collection of data. For example, more could be done to promote the option to use individual paper and online forms.
APP 4 – Dealing with unsolicited personal information	**Compliant**	Some unsolicited personal information may be provided, particularly during field work. ABS privacy training includes coverage of this issue. ABS has appropriate measures in place to handle the receipt of unsolicited information.	–
APP 5 – Notification of the collection of personal information	**Action required**	The ABS is drafting a new privacy notice for the 2021 Census. During the development of this PIA, Galexia has provided input on key issues that have now been addressed in the new draft privacy notice (Refer to APP 5. Notification issues resolved). One outstanding issue is that APP 5 requires consumers to be informed about the consequences of not providing information. This is a complex issue for the Census and requires careful consideration. Completing the Census is mandatory, but there are only potential consequences once an individual has received a formal Notice of Direction. The ABS has to tread a fine line between encouraging participation and providing realistic information about the consequences for not responding. ABS is generally compliant with the other requirements of APP 5.	Recommendation 3: **Clarify privacy notice information on the potential consequences for not providing information** The ABS should develop a clear and consistent set of wording to inform consumers about the consequences of not completing the Census.

APP 6 – Use or disclosure of personal information	**Compliant**	APP 6 generally allows the use and disclosure of information, including sensitive information, where a legal authority exists for that use or disclosure. This rule applies to the use and disclosure of Census data (e.g. for statistical publications and data integration projects), but is 'trumped' by the more restrictive provisions of the Census legislation. Under the Census legislation, the ABS cannot release information that is likely to identify an individual. Some external stakeholders have raised concerns regarding the methods that ABS uses to de-identify information before publishing reports or making data available to researchers. However, this PIA recommends that the ABS continues to use its current 'layered approach' to managing re-identification risk. This PIA makes some suggested enhancements to this approach in Structural Recommendation 3: Principles based approach to managing re-identification risk	–
APP 7 – Direct Marketing	**Compliant**	The ABS is prohibited from releasing information that is likely to identify an individual. APP 7 is not relevant to ABS activities in relation to the 2021 Census.	–
APP 8 – Cross-border Disclosure	**Compliant**	The ABS does not process, store or transfer any information from the 2021 Census outside Australia. The ABS has included a prohibition on cross-border data transfers in its agreements with third party service providers. The ABS is compliant with APP 8 in relation to the 2021 Census.	–
APP 9 – Government Related Identifiers	**Compliant**	APP 9 has very limited application to the 2021 Census. Government related identifiers do not play a direct role in the collection, use and disclosure of information in the Census. However, the 2021 Census dataset will be used in data integration projects such as the Multi-Agency Data Integration Project (MADIP). MADIP uses government related identifiers as part of its identity linking process. This use is compliant with APP 9, as the restrictions in APP 9 only apply to private sector organisations.	–
APP 10 – Quality of Personal Information	**Compliant**	Data quality is an important issue for the Census. A Post Enumeration Survey is conducted after each Census and a report on Data Quality is published. The 2016 Census Data Quality report found that data quality was acceptable for the objectives of the ABS and its clients. Lessons learned from that report are being implemented by the ABS for the 2021 Census.	–

APP 11 – Security **(Independent Security Risk Assessments)**	**In progress**	The data being collected, used and disclosed in the 2021 Census includes highly sensitive data. The scale of the data involved is also significant. It will be important for security settings to match the potential harm of any breaches. ABS updated the *2021 Census – Security Strategy (IT Security)* in January 2020. This provides a high level approach to identifying and managing security risks. ABS has not undertaken a comprehensive independent security risk assessment for the 2021 Census as of April 2020, although an 'end to end' security risk assessment has been commissioned. During the development of this PIA, Galexia has recommended that further specific security risk assessments be conducted on two key areas: • The Cloud platform; and • The Time Capsule.	**Recommendation 4: Conduct independent security risk assessments for key 2021 Census components** The ABS should commission independent security risk assessments for key components of the 2021 Census: • An 'end to end' assessment (this has been commissioned); • A specific assessment of the cloud platform (this may be covered by existing security certifications); and • The Time Capsule (this has not been commissioned).
APP 11 – Security **(Data Retention – Names)**	**Action required**	APP 11 requires the ABS to destroy or de-identify data as soon as there is no business purpose for retaining it. This is also best practice in reducing the security risk profile of large datasets. During discussions with ABS teams during the development of this PIA it has become clear that the time required for keeping names could be much shorter. Names are useful in reconciling duplicates and gaps in coverage and play an important role in data quality. (Refer to the 2021 Census Privacy Statement[3] for examples of how the ABS uses name and address information.). The long-term retention of names does however present an unacceptable level of privacy and security risk for the Census, and may undermine other privacy measures.	**Recommendation 5: Shorten data retention periods for names** The ABS should review and significantly reduce the data retention periods for names. If the reduction needs to be staggered to meet business needs, this should be reduced over the next two Censuses. As a minimum the data retention period for names should be re-set as 18 months for the 2021 Census.
APP 11 – Security **(Data Retention – Addresses)**	**Action required**	Retention of address data may provide some additional assistance in Census planning and data quality measures. But again, no justification was presented for the long-term retention of all addresses. The long-term retention of addresses does however present an unacceptable level of privacy and security risk for the Census, and may undermine other privacy measures.	**Recommendation 6: Shorten data retention periods for addresses** The ABS should review and, if possible, reduce the data retention periods for addresses. If the reduction needs to be staggered to meet business needs, this should be reduced over the next two Censuses. As a minimum the data retention period for addresses should be reduced for the 2021 Census to a period of 24-36 months.

[3] The Privacy Statement will be available at <www.census.abs.gov.au/privacy> from mid-October 2020. During the PIA process the Census Privacy Team conducted an investigation into the length of time names and addresses are proposed to be retained by the ABS from the 2021 Census. Teams undertaking core Census activities, data integration and other activities that rely on names and addresses from the Census identified how the names and/or addresses are used, and the length of time taken to complete these activities.

ABS considered:

- Census activities that include coding and processing to produce Census data for release to the public and internal activities to prepare for the next Census including updating of indexes and system testing.
- Other (non-Census) teams which use either names and/or addresses for a range of activities including data integration and input to Closing the Gap reporting.

APP 12 – Access **(General access rules)**	**Action required**	ABS has access policies and procedures in place for its own data that are compliant with APP 12. ABS also has a special *Privacy Act 1988* and *Freedom of Information Act 1982* exemption available for access requests in relation to data that it has collected for statistical purposes. However, in relation to the 2021 Census there is a lack of clarity over what data may be the subject of access requests (noting that exemptions are clearly available for access to some of these datasets, but these exemptions are not currently mentioned in the ABS Privacy Policy[4]).	Recommendation 7: **Clarify access rules for different categories of data** The ABS should clarify the access rules that apply to each category of data, and set these out clearly in the ABS Privacy Policy, including: • Core Census data (i.e. statistical data); • ACLD; • Integrated Census data (e.g. MADIP); • Time Capsule; and • Other non-statistical data (e.g. Contact Centre records).
APP 12 – Access **(Time Capsule access rules)**	**Action required**	Rules around access to Time Capsule data may need to be clarified and strengthened following recent international experiences, where pressure has been applied for early access to Time Capsule data.	Recommendation 8: **Clarify and strengthen access restrictions to data held in the Time Capsule** The ABS should clarify and strengthen access rules that apply to data held in the Time Capsule, noting examples of international pressure for early access to similar data.
APP 13 – Correction	**Compliant**	ABS has access policies and procedures in place for its own data that are compliant with APP 13.	–

2.6. ABS Legislation

This PIA also assesses the 2021 Census implementation against ABS legislation.

The following table summarises high level findings on compliance with ABS legislation:

ABS Legislation	Action / Status	Galexia Commentary
Census and Statistics Act 1905 (Cth)	**Compliant**	General Census use and disclosure must comply with the objectives of the Act. Section 8 of the Act specifically authorises the Census. Section 8a authorises the Time Capsule. The Act contains a prohibition on releasing any data in a manner that is likely to enable the identification of a particular person. The Act also contains significant penalties and sanctions for releasing data. The ABS has taken steps to ensure that all persons and partners engaged in the Census are covered by these provisions (for example, field workers become temporary employees of the ABS).
Australian Bureau of Statistics Act 1975 (Cth)	**Compliant**	The Act allows the ABS to both collect data and integrate data with other data holdings (Section 6). This is the basis for the participation of Census data in the Multi-Agency Data Integration Project (MADIP).

Refer to Section 20. ABS Legislation for further information.

[4] ABS, *Privacy Policy* (6 January 2020) <www.abs.gov.au/websitedbs/D3310114.nsf/Home/Privacy+Policy>

2.7. Australian Government Agencies Privacy Code

The *Australian Government Agencies Privacy Code* (the Code) was registered on 27 October 2017 and commenced on 1 July 2018 <www.oaic.gov.au/privacy-law/australian-government-agencies-privacy-code>.

The following table summarises the key privacy governance obligations contained in the Code:

APS Privacy Code Requirements	APP Code Section	Action / Status	APS Privacy Code Detailed Requirements	Galexia Commentary and Recommendations
A. Privacy Management Plan	**9**	**Compliant**	An agency must have a Privacy Management Plan that: – identifies specific, measurable privacy goals and targets; and – sets out how an agency will meet its compliance obligations under APP 1.2.	A comprehensive Privacy Management Plan has been published. However, the Plan covers the ABS as a whole, and is not specific to the Census. This PIA recommends that the ABS adopts a new 7-8 year Census Privacy Strategy, covering more than one Census period. Refer to Structural Recommendation 1: Census Privacy Strategy
B. Privacy officer	**10**	**Compliant**	An agency must appoint a Privacy Officer.	A Chief Privacy Officer has been designated and plays an active role in 2021 Census planning, implementation and oversight.
C. Privacy champion	**11**	**Compliant**	An agency must appoint a senior official as a Privacy Champion.	An ABS Privacy Champion has been in place for two years and plays an active role in 2021 Census planning, implementation and oversight.
D. PIAs	**12**	**In Progress**	An agency must undertake a written Privacy Impact Assessment (PIA) for all 'high privacy risk' projects.	ABS undertakes regular PIAs. During the development of this PIA, Galexia identified two areas where some further work could be considered. **Recommendation 9: Conduct additional independent PIAs for activities that are 'renewed' for each Census** The ABS should consider conducting additional independent PIAs for the ACLD and the Time Capsule.
E. PIA register	**15**	**Compliant**	An agency must keep and publish a register of all PIAs conducted.	The ABS maintains a public PIA Register.[5]
F. Privacy training	**16**	**Compliant**	An agency must enhance internal privacy capability.	ABS has comprehensive policies and procedures in place on privacy training, awareness raising and capacity building.
G. Monitoring and review	**17**	**Compliant**	An agency must regularly review and update its privacy practices, procedures and systems.	In addition to the general ABS Privacy Management Plan (which is monitored and reviewed every year), the Census has its own High Level Privacy Work Plan that is monitored and reviewed six-monthly.

Refer to Section 21. Australian Government Agencies Privacy Code for further information.

[5] <www.abs.gov.au/websitedbs/D3310114.nsf/home/ABS+Privacy+Impact+Assessments>

2.8. Additional Governance Requirements

The ABS is subject to more than compliance with the APPs, so a broader governance framework is required.

The following table summarises (briefly) the core requirements that should be included in the ABS governance arrangements for the 2021 Census.

Additional Governance requirement	Action / Status	Galexia Commentary	Galexia Recommendation
A. Explaining the legal basis for data linkage	**Compliant** **Further measures possible**	The governance arrangements for the use of Census data in data integration are largely set out in MADIP policies and procedures. However, one area of potential weakness is that the ABS policy on restricting linking Census data from prior Census collections (e.g. longitudinal study) via MADIP is not easily located. This policy should be prominent on information pages about both MADIP and the Census.	Recommendation 10: **Clarify the prohibition on using multiple Census collections in MADIP** The ABS should clarify and highlight the prohibition on using multiple Census collections for longitudinal study via MADIP.
B. Managing agreements with third parties and contractors	**In progress**	The ABS will be working with numerous third parties / contractors / partners for the implementation of the 2021 Census. Managing multiple third parties in a complex project can lead to privacy and security risks. During the PIA process, the ABS was advised that the 2021 Census would benefit from the establishment of an internal register of all third parties. The ABS will be able to use the Register to drive consistently high standards across agreements.	Recommendation 11: **Establish and maintain a register of third party agreements** The ABS should establish a register of third party agreements and use this to drive / promote a consistently high level of privacy protections and privacy management. **Note:** Work has commenced on this register and the issue is marked as 'in progress'.
C. Managing Function Creep Legislative basis for use of data	**Action Required**	The core question is not to identify the legal basis for *collecting* the data in the Census, but to place appropriate limits around what the data can then be *used* for. It is important for ABS to modernise its core legislation and add a specific section outlining the permitted and prohibited uses for the data that it collects.	Recommendation 12: **Clarify ABS legislation to set out permitted and precluded purposes for use of Census data** The ABS should explore ways to clarify legal restrictions on the use of Census data. Options might include a guideline, declaration or a potential legislative amendment.
D. Managing Function Creep Application of the DATA Framework	**Action Required**	Confidence in the privacy protections built into the Census may potentially be impacted by relying on the proposed DATA Framework to share or release data. That framework 'trumps' secrecy provisions in existing legislation, unless an Agency has succeeded in excluding itself from the framework. ABS is yet to establish a formal position on its involvement in the DATA Framework. Use of the DATA Framework would be so different to normal ABS requirements that the recommendations in this PIA would not be applicable.	Recommendation 13: **Clarify the relationship between Census data and the proposed Data Availability and Transparency (DATA) Framework** The ABS should consider whether or not to exclude Census data from the proposed DATA Framework, and the potential impact of the DATA Framework on both the generic secrecy provisions that apply to ABS data and the specific privacy protections that apply to Census data.

E. Managing Function Creep Application of the DATA Framework to the Time Capsule	**Action Required**	One specific impact that should be the subject of further examination is the potential for the DATA Framework to over-ride the specific secrecy provisions that apply to the Time Capsule. Any attempt to use the DATA Framework to gain early access to Time Capsule data represents an unacceptable risk to privacy, and a significant risk to the reputation of the Census. It may be sensible for the ABS to seek a specific exemption from the DATA Framework for the Time Capsule.	**Recommendation 14: Seek an exemption from the proposed DATA Framework for the Time Capsule** The ABS should seek an exemption for the Time Capsule from the proposed Data Availability and Transparency (DATA) Framework. This recommendation should be seen as the minimum ABS response to the proposed DATA Framework, and not the full response.
F. Managing Function Creep Inclusion of health information in the Time Capsule	**Action Required**	The inclusion of health information in the Time Capsule is high risk, as the Time Capsule is released as raw / identified data. Although Time Capsule data is not released until 99 years after it is collected, the inclusion of health information could have a potential impact on individuals. The presence of certain health conditions in individuals as revealed by the Time Capsule, might indicate the potential presence of genetically inherited conditions in their descendants. Removing the health data would reduce the overall security risk of the Time Capsule, as well as reducing any potential negative impacts from genetic profiling.	**Recommendation 15: Remove the new health data collected in the 2021 Census from data submitted to the Time Capsule** The ABS should ensure that responses to the new long-term health conditions question are not included in the Time Capsule, and that this is clearly explained to consumers.
G. Reviewing the consequences for not responding to a Notice of Direction	**Action Required**	This PIA raises some concerns over the consequences for failing to respond to a Notice of Direction. Awareness of privacy, attitudes to data, and trust in government are all changing. The idea that an individual might end up with a criminal record for having strong concerns about privacy appears harsh, and the detriment to the overall Census may not justify the continuation of the traditional approach to refusals and prosecutions. This PIA includes a Recommendation for ABS to reform the refusals and prosecution process to implement a better balance between response rates and consequences for individuals facing prosecution.	**Recommendation 16: Review the consequences for refusing to complete the Census** The ABS should reform the refusals and prosecution process to implement a better balance between response rates and consequences for individuals facing prosecution. However, as it is unlikely that this issue can be resolved in time for the next Census, Galexia recommends that the proposed Census Privacy Strategy should include a review of the refusals and prosecution process for non-completion of the Census (Refer to Structural Recommendation 1: Census Privacy Strategy).

Refer to Section 22. Additional Governance Requirements for further information and detailed discussion.

2.9. Social Licence

One of the aims of the overall ABS Privacy Management Plan is to build a social licence for activities such as the 2021 Census.

In order to develop the social licence for the 2021 Census, ABS needs to take measures to address each of these following components:

Social Licence Requirements	Action / Status	Galexia Commentary	Galexia Recommendation
A. A sound basis for believing in the integrity and accountability of the ABS	**Action required**	Generally the ABS is a trusted and respected organisation. However, confidence in the Census was shaken by key events in relation to the 2016 Census. The conduct of this independent PIA and the implementation of the recommended steps in this PIA (especially major changes such as reducing data retention periods) should help to restore community trust in the ABS.	This issue should be addressed by: • Structural Recommendation 1: Census Privacy Strategy; and • The two Recommendations on data retention: – Recommendation 5: Shorten data retention periods for names; and – Recommendation 6: Shorten data retention periods for addresses.
B. Consumers feel they have some control over how their own data is used and by whom	**Action Required**	There are two key challenges in providing consumers with confidence over how their Census data is used: • **Data retention** – Names and addresses collected in the Census are currently held for too long; and • **Data linkage** – The data linkage process is difficult for consumers to understand and there is a significant amount of incorrect information related to ABS data linkage processes in online commentary.	Both of these issues should be addressed by: • Structural Recommendation 1: Census Privacy Strategy; • Structural Recommendation 2: Principles based approach to name encoding for data linkage; and • The two Recommendations on data retention: – Recommendation 5: Shorten data retention periods for names; and – Recommendation 6: Shorten data retention periods for addresses.
C. Consumers have the ability to choose to experience some of the benefits of data use themselves	**Compliant**	Consumers are likely to accept that some of the benefits of the Census are available for them to choose as individuals, such as data on education and transport.	–
D. Consumers understand the potential community-wide benefits of data use	**Compliant**	Consumers generally recognise the community-wide benefits of the Census, particularly in relation to the provision of government services and the management of elections. The inclusion of Indigenous data is also recognised as a significant community benefit.	–

Refer to Section 23. Social Licence for further information and detailed discussion.

2.10. Galexia Privacy Risk Identification

This PIA includes a summary privacy risk assessment, following earlier work on risk during the PIA process.

The following table is a summary of risk gradings by theme. Refer to Section 24. Galexia Privacy Risk Identification for the summary Galexia risk assessment and mapping to recommendations.

Privacy Risk Summary	High	Medium	Low	Grand Total
Data minimisation		1		**1**
Data retention	1	1		**2**
Function creep	1	4		**5**
Governance	6	1		**7**
non-response			1	**1**
Openness	2			**2**
Re-identification		3		**3**
Reduced Trust		1		**1**
Security breach	6	1	1	**8**
Third party collection	2	1		**3**
Trigger questions		2		**2**
Grand Total	**18**	**15**	**2**	**35**

2.11. Employee Data

Employee data is also **briefly** covered in this PIA, but in order to aid clarity the employee data section appears in an Appendix (Refer to Appendix E – Employee Data).

Employee data, for the purposes of this PIA means data such as:

- Data relating to ABS **employees** engaged in Census activities; and
- Data relating to ABS **contractors** engaged in Census activities.

This PIA includes one recommendation on employee data:

Australian Privacy Principle (APP)	Action / Status	Employee Data	
		Galexia Commentary	Galexia Recommendation
APP 11 – Security	**In progress**	**General security** The agreement with Adecco includes extensive security requirements relating to IT security, physical security, data breaches and return of ABS information at the conclusion of the contract. **App security** The MyWork App collects and shares some employee data, including potential information on location and movements. The App should be the subject of an independent security review.	Recommendation 17: **Conduct an Independent security review for the MyWork App** The ABS should commission an independent security risk assessment for the proposed MyWork App. **Note:** This review will be scheduled by the ABS.

3. Census Overview

3.1. ABS Overview

The ABS is Australia's national statistical agency, providing statistics on a wide range of economic, social, population and environmental matters of importance to Australia.

The ABS is subject to significant confidentiality provisions contained in various legislation. The most relevant include:

- *Australian Bureau of Statistics Act 1975* (Cth);
- *Census and Statistics Act 1905* (Cth); and
- *Privacy Act 1988* (Cth) and Australian Privacy Principles (the APPs).

3.2. Data Flows – Core Census activities

The Census is a national survey that collects data from all persons in Australia on Census night. The Census is conducted every five years and the next Census will be held in August 2021.

The Census can be completed online or on a paper form. The majority of consumers are expected to complete the 2021 Census online.

A key feature of the Census is that both the paper form and the online form can be completed for a household. One person can submit information about everyone in the household. In practice, some households will delegate this entire task to an individual. Other households will pass the form from person to person (or take turns using the online service) until the form is complete.

An individual may choose to complete their own form, even if they belong to a household group. However they have to contact the ABS to request an individual form. Where they complete both a household form and an individual form, the data from the individual form is used in the Census. In the 2016 Census fewer than 100,000 individuals requested an individual form [Note: this may include some households where an additional form was required because more than six individuals resided there on Census night (the paper household form only had six columns)].

The bulk of Census data is derived from completed forms. However, in order to support the administration of the Census, a range of additional data may be collected regarding consumers. Examples include:

- Gathering address details from multiple sources in order to manage mail-outs and field work (the ABS maintains a national Address Register[6]);
- Receiving direct inquiries from consumers via correspondence, via the Contact Centre or via Census online self-service options – including an online chatbot;[7]
- Gathering some consumer information from third parties in limited circumstances, such as gathering data on inmates from the authorities running correctional facilities;
- Re-contacting selected households for a quality assurance survey that is conducted several months after the completion of the Census in the Post Enumeration Survey;[8] and

[6] The Address Register was established by the ABS in 2015 as a comprehensive list of all physical addresses in Australia. The Address Register Common Frame is a comprehensive data set of Australian address information. It contains current address text details, coordinate reference (or 'geocode'), and address use information for addresses in Australia.

[7] In the 2016 Census the ABS Contact Centre received 3.4 million calls from members of the public.

[8] Refer to:

- ABS, *2901.0 – Census of Population and Housing: Census Dictionary, 2016* (19 October 2017) – **Post Enumeration Survey (PES)** <www.abs.gov.au/ausstats/abs@.nsf/Lookup/2901.0Chapter47502016>.
- ABS, 2940.0 – Census of Population and Housing: Details of Overcount and Undercount, Australia, 2016 (22 June 2017) – **About the Census Post Enumeration Survey** <www.abs.gov.au/ausstats/abs@.nsf/Lookup/by%20Subject/2940.0~2016~Main%20Features~About%20the%20Census%20Post%20Enumeration%20Survey~2>

- Potentially using some administrative data to support Census operations, such as using external data sources data to identify unoccupied buildings. Note: The potential use of administrative data to support the Census is covered in detail in a separate PIA on that issue, and is not discussed in detail in this PIA. The ABS maintains a public PIA register where the PIA on administrative data can be accessed.[9]

This PIA concentrates on the core statistical data collected from consumers via the Census form, but notes other information flows where they are relevant to a specific privacy issue.

Participating in the Census is mandatory. The Census is conducted under the authority of the *Census and Statistics Act 1905 (Cth)*.[10] If an individual refuses to complete a Census form, the Australian Statistician has the power to direct them to do so. The ABS always seeks 'willing participation' first, but if an individual fails to respond to a formal direction, they may face serious legal consequences.

Most Census questions are also mandatory. However there are some limited exceptions:

- Consumers can complete either their date of birth ***or*** their age; and
- The question on religious beliefs is marked as optional[11] (over 90% of consumers completed that question in the 2016 Census).

Census questions also differ slightly from other general surveys conducted by organisations other than the ABS, in that there is no option to state 'not known', 'unsure', or 'prefer not to say' when responding. The ABS explains that their overall level of data accuracy is higher when consumers provide an approximate answer, rather than ticking a box such as 'not known'.

The Census process begins with the ABS delivering every household a Census form or a letter inviting them to complete the Census online. The letter and the form include a unique code (**Census Number**)[12] which is linked to the address of the target household. The letter contains another unique code (**a temporary password**) which is provided so that users can login and complete the Census online. The unique codes for every paper form and eForm also help the ABS to avoid multiple form submissions from the same household (or to reconcile any multiples that are received). They also help the ABS to follow-up households where no form is submitted.

The following diagram provides a high level overview of the practical implementation of the Census:

[9] <www.abs.gov.au/websitedbs/D3310114.nsf/home/ABS+Privacy+Impact+Assessments>

[10] <www.legislation.gov.au/Details/C2016C01005>

[11] Refer to Appendix B – Extracts from the Census Test Forms for an example.

[12] The **Census Number** will be applied to the digital service, letters, paper forms and customer support services (e.g. sms and support centre). Additionally there may be a:

- **Temporary password** – provided by the ABS, so that users can login and complete the Census online
- **Password** – established by the user.

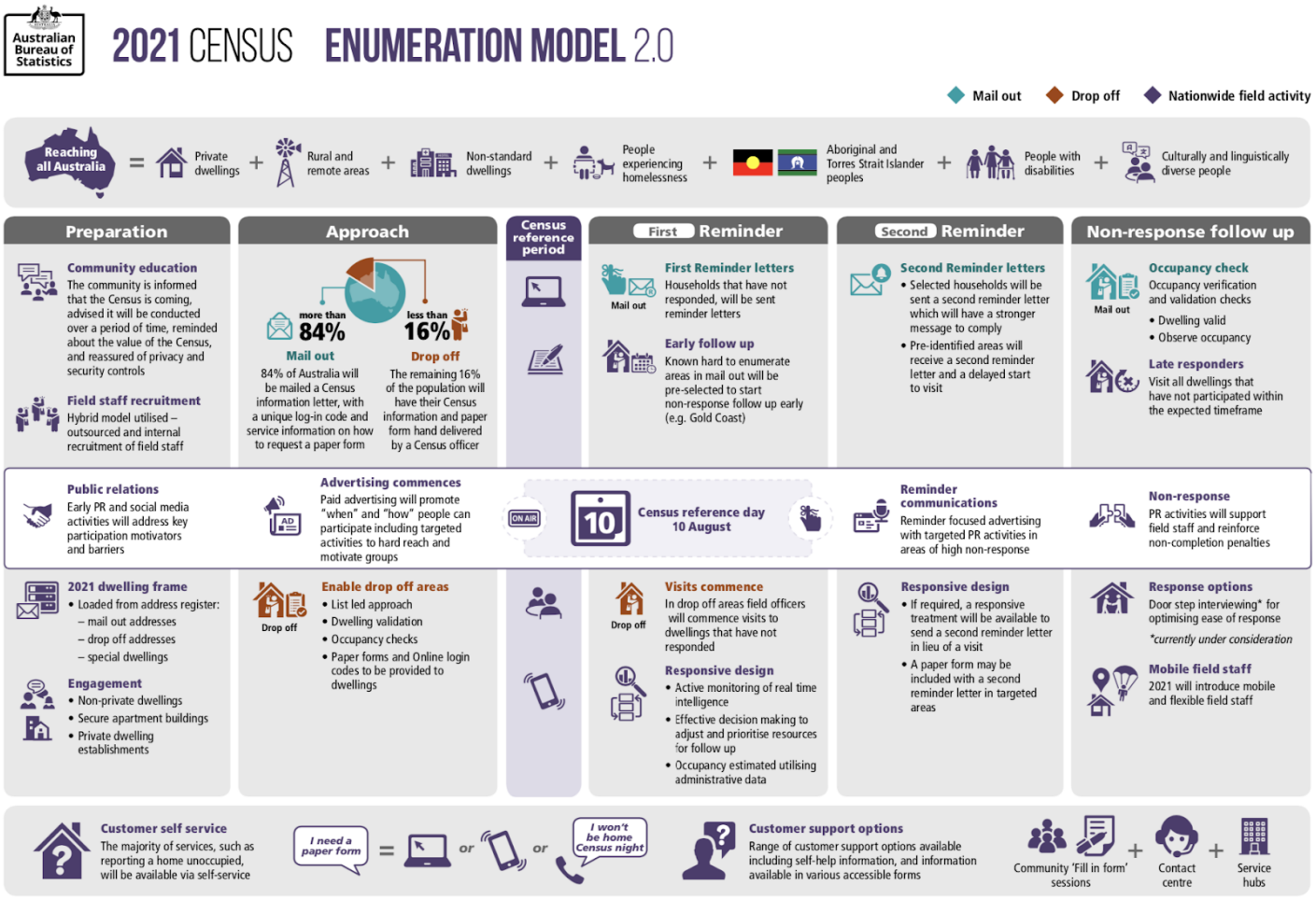


Diagram: 2021 Census Enumeration Model 2.0 – February 2019 (supplied by ABS)

In practice approximately 75% of households will complete the Census online. This leaves around five million paper forms that will be submitted by post. When paper forms are received, the name and address details are separated from the other content, so that ABS staff conducting data entry or coding only see the information that is specific to their task. Data from the online and paper processes is eventually combined and reconciled in the Enumeration Management System (EMS). Again, the EMS maintains strict separation of name and address data from other Census content.

Overall, approximately 95% of consumers complete the Census (in 2016 the response rate for individuals was 94.8% and the response rate for occupied households was 95.1%). The ABS is able to impute some data for households that failed to complete the Census (e.g. by using data from similar households on key demographics such as age and gender) – even using this technique the Census undercounts the population by a small amount. In the 2016 Census the net undercount was estimated at 1%.[13]

[13] Census Independent Assurance Panel (CIAP) to the Australian Statistician, *Report on the Quality of 2016 Census Data* (July 2017) <www.abs.gov.au/websitedbs/d3310114.nsf/Home/Independent+Assurance+Panel>.

Once the data has been submitted, there are four Information 'pathways' for Census data:

1) **Core Census products**[14]
Core Census products include statistical publications and data products that are made available to the research community. A key ABS data product is TableBuilder which allows researchers to query a small sample of the underlying Census data using an online service (for low risk data) or via a secure data lab (for higher risk data). Core Census products such as statistical publications use up to 100% of the data collected in the Census. All core Census products are subject to a de-identification requirement (discussed in more detail later in this PIA);

2) **Data integration**[15]
Census data can be integrated with other government data sets for policy analysis, research, and statistical purposes via data integration projects such as the Multi-Agency Data Integration Project (MADIP).[16] Integrated datasets are subject to data minimisation constraints for each research project, so will only contain the necessary Census data items for the required demographic or geographic group needed to answer the research question. Encoded personal identifiers (such as name) are used to facilitate data integration, but any Census data included in an integrated dataset is de-identified. This encoding approach is discussed in more detail later in this PIA;

3) **Census Time Capsule**[17]
The Census Time Capsule is a full copy of the Census forms completed by some individuals who have chosen to participate. It is held by the National Archives of Australia (NAA) and only released after 99 years. Unlike other Census related datasets the Time Capsule includes name and address. About 50% of consumers agreed to have their data included in the Time Capsule in the 2016 Census. Once released, the data is typically used by historians and genealogists; and

4) **Australian Census Longitudinal Dataset (ACLD)**[18]
This dataset covers a 5% random sample of data subjects, and provides a longitudinal dataset covering multiple Censuses. Researchers wishing to conduct longitudinal studies of Census data can only use the ACLD dataset – no longitudinal study is allowed under core Census products or data integration programs such as MADIP. Data from each Census is linked using a name encoding process and only de-identified data is made available to researchers. Individual consumers are not informed whether or not their data is included in the 5% sample used in ACLD.

The collection of data on the Census forms (paper and online) is only the start of a complex data flow. The raw information needs to be reconciled, processed and categorised, before it is disseminated to the four data pathways described above. This process is described in the diagram on the next page:

[14] <www.abs.gov.au/websitedbs/D3310114.nsf/home/census>

[15] <www.abs.gov.au/websitedbs/D3310114.nsf/Home/Statistical+Data+Integration>

[16] MADIP is the subject of a separate PIA and is not discussed in detail in this report. ABS maintains a public register of PIAs at <www.abs.gov.au/websitedbs/D3310114.nsf/home/ABS+Privacy+Impact+Assessments>

[17] <www.abs.gov.au/ausstats/abs@.nsf/Lookup/by%20Subject/2008.0~2016~Main%20Features~Census%20Time%20Capsule~143>

[18] <www.abs.gov.au/ausstats/abs@.nsf/mf/2080.0>

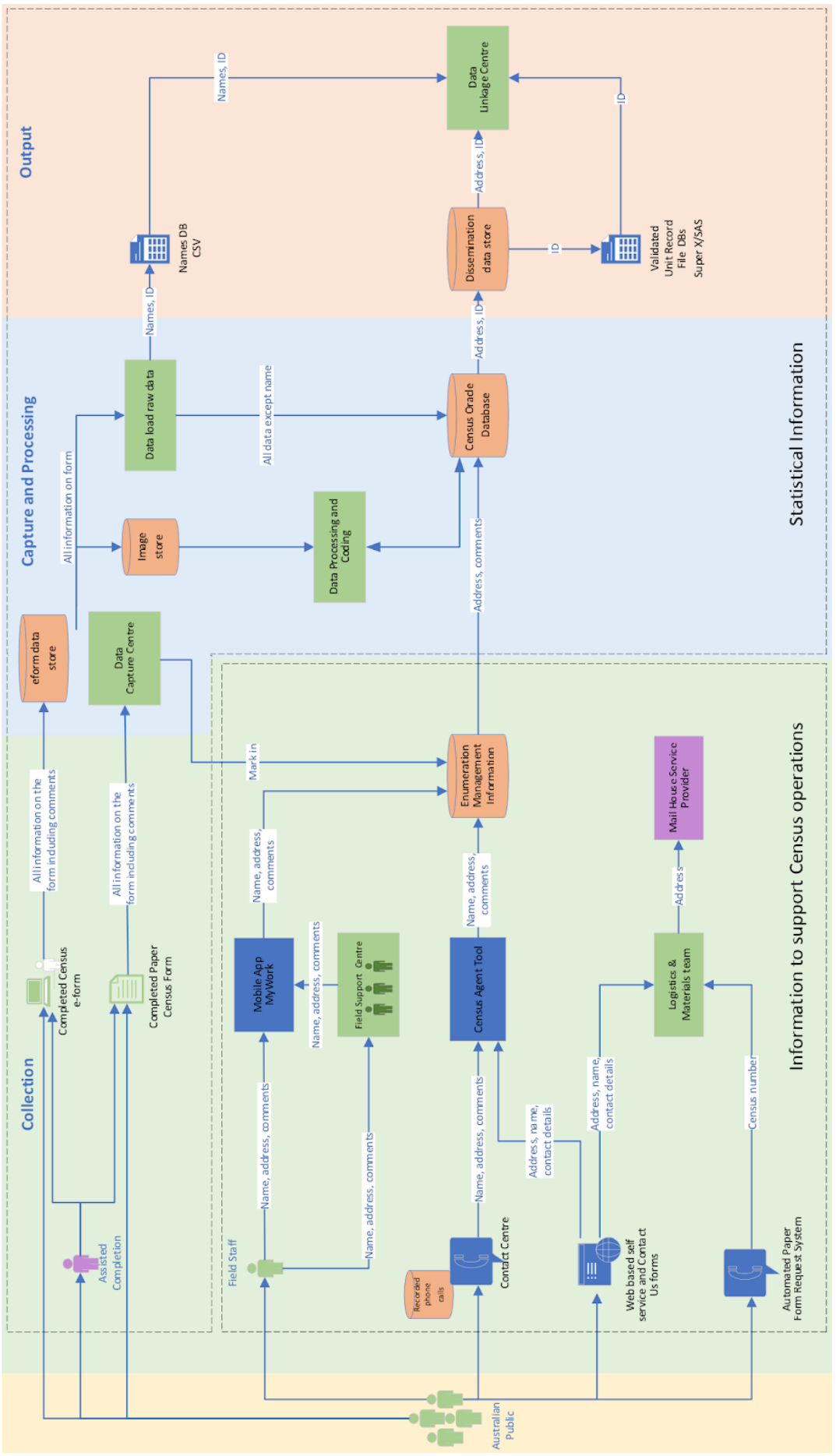
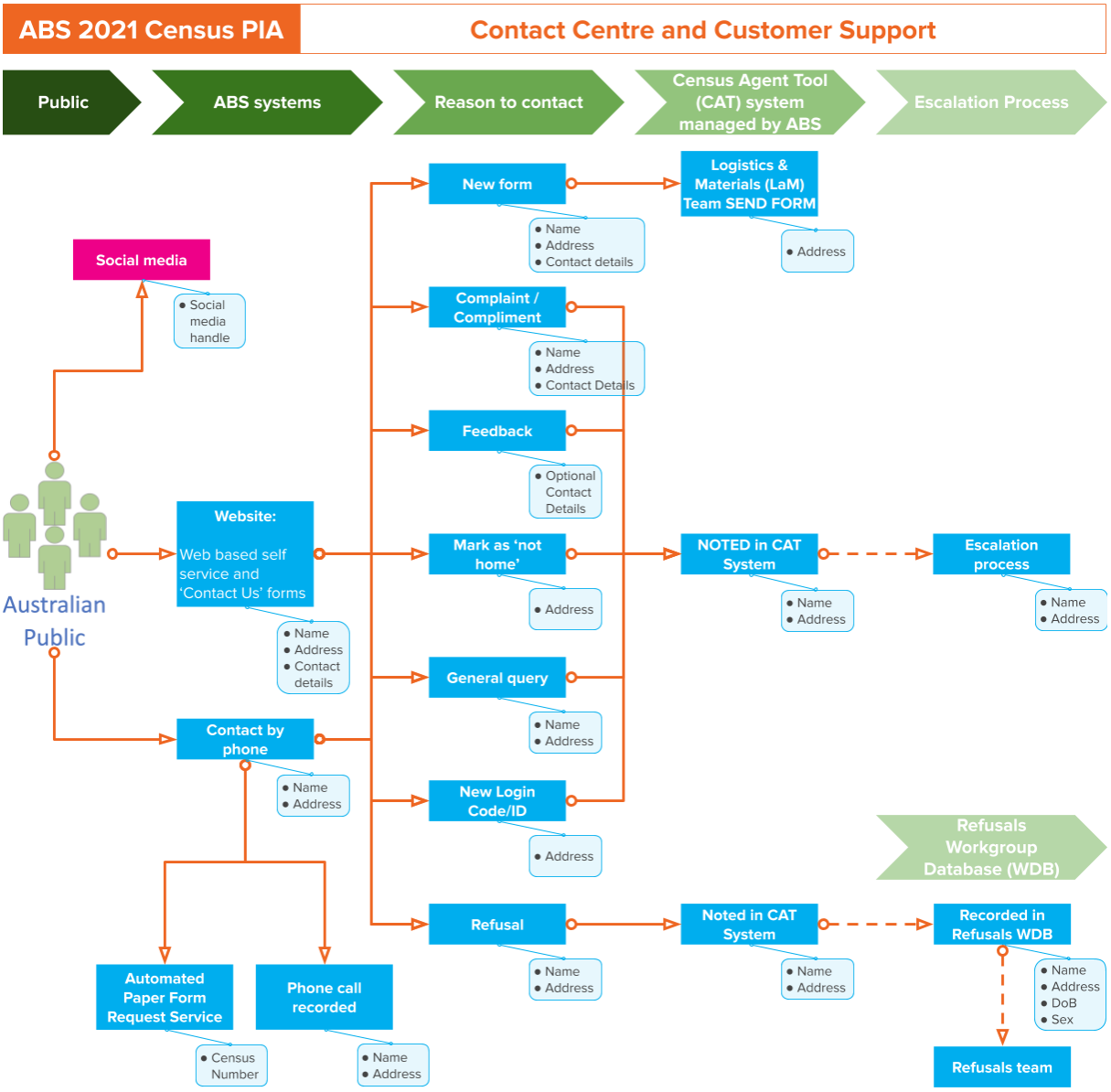


Diagram: Census Enumeration and Processing Flow – Personal and Sensitive Information – April 2020 (supplied by ABS)

The main components of the Census implementation set out in the data flow diagram above are summarised in the following table:

Entity	Role
Field Officer	Field Officers drop off, follow-up and collect Census forms from the Australian public.
Contact Centre	The Contact Centre uses an Interactive Voice Response (IVR) system to initially answer and direct calls. There is an MoU in place with Services Australia to assist in the provision of the Contact Centre. Both ABS and Services Australia staff will be answering calls. Calls will be recorded.
Census Agent Tool (CAT)	Information is captured by Contact Centre staff using the Census Agent Tool (CAT). Contact Centre staff could be provided with the following information: ● name, ● address, ● email, ● phone number, ● relationship of respondent to dwelling, ● number of people in the dwelling. Information collected is used to identify the dwelling so the outcome can be recorded against the unit record (e.g. not at home on Census night).
Web based self-service forms	The Australian public can enter a request into a self-service form to ask for assistance such as a paper form or a new Census Number. Name, address and mobile phone numbers may be collected during this process.
Paper form request	An IVR system can be called to request a paper form to be posted out.
Logistics and Materials (LaM) team	The Logistics and Materials team have address information for all dwellings in mail out areas (a dwelling may receive a form or letter). They also receive address information for Paper Form requests (residents requesting paper form). This team is also responsible for sending paper materials to Field Officers.
Mail house service provider	The mail house service provider will use the address to send the requested paper form. Logistics and Materials team supply encrypted address files to contractors. Contractors are required to destroy all paper/online information by November 2021.
Field Support Centre (FSC)	Field Support will have access to information on persons recruited to work in the FSC and Field Officers who will collect Census forms and return them to the ABS.
Mobile App	Field Officers use a mobile app – **the MyWork App** – to communicate with Census Management. They will have secure devices with which to communicate which may be their own mobile phones or tablets.
Enumeration Management Information (EMI)	The EMI is the data store holding operational data such as names, addresses, emails, and phone numbers.

Some additional information flows occur outside the core enumeration process. These include contacts from members of the public described in the diagram below:



Although a significant majority of consumers complete the Census on Census night, some individuals are slower to complete the process or return the forms and require follow-up. A small group of individuals never complete the Census.

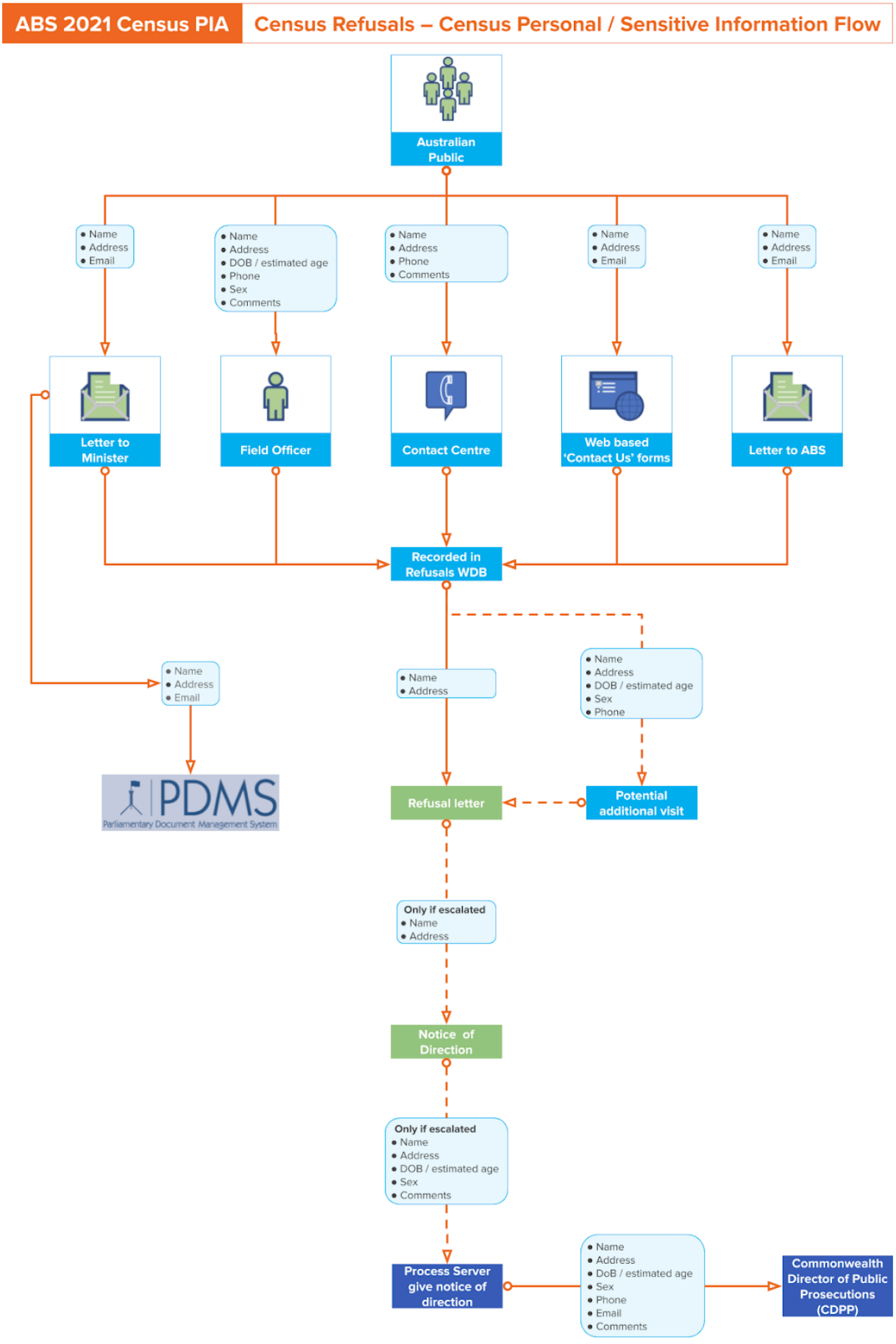
The ABS uses the term 'refusals' to describe a wide range of activities related to individuals who initially fail to complete a Census form, and we use the term in this PIA. This is one area where the ABS may use name and address details more extensively than in other Census activities, especially where a formal notice is issued to an individual, or legal proceedings are commenced.

In the 2016 Census approximately 10,000 households that failed to complete the Census were escalated to the formal category of 'refusals' at the ABS. This resulted in the following actions:

1) 4,607 refusal letters were sent to households;
2) 2,969 formal Notices of Direction were issued;
3) Approximately 40 matters referred by the ABS to the Prosecution Service; and
4) Approximately 17 court matters resulted in a fine or conviction.

The number of follow-up actions diminishes at each stage because households comply, or more information becomes available regarding their circumstances.

The data flows in the refusals process are quite complex, and are set out in the following diagram:



3.3. Benefits of the Census

The ABS summarises the benefits of the Census as follows:

> Information from the Census helps governments, businesses and not for profit organisations across the country make informed decisions. The Census improves the accuracy of population estimates for Australia in each state, territory, and local government area. It informs decisions on electoral boundaries and underpins funding to states, territories and local governments. It informs decisions for services and infrastructure such as roads, childcare, hospitals and schools for every community in Australia. The Census is also a vital tool for a myriad of investment decisions made by businesses across all sectors of the economy, and is used by community groups to inform support for some of the most vulnerable people in Australia.[19]

A 2019 report on the value of the Census concluded that the Census delivers a national benefit of over $800 million per year, or around $6 in benefit for every $1 that it costs to run.[20]

[19] ABS, *Planning the Census 2021* <www.abs.gov.au/ausstats/abs@.nsf/mf/2089.0>

[20] Lateral Economics, *Valuing the Australian Census* (August 2019) <www.abs.gov.au/websitedbs/D3310114.nsf/home/Value+of+the+Australian+Census>

4. Privacy Strengths and Weaknesses

Galexia considers the proposed design of the 2021 Census delivers a mix of privacy strengths and weaknesses – set out briefly below, and further information is provided in the relevant sections later in this report.

Strengths

- The ABS is subject to a legislative prohibition on releasing any data that might lead to the identification of an individual (contained in the *Census and Statistics Act 1905* (Cth));
- Penalties and sanctions, including imprisonment and hefty fines, are in place for any unauthorised access to Census data or inappropriate use of the data;
- The ABS has strong IT systems and security in place, including processes for detecting misuse of information by ABS staff and users of statistical information;
- The objectives and likely outcomes of the 2021 Census are clearly in the public interest and are likely to deliver significant community benefit;
- The ABS has invested heavily in privacy training and capacity building; and
- The ABS recognises the importance of privacy – the ABS Census Privacy team has been in regular communication with the OAIC and is committed to an independent PIA process.

Weaknesses

- The level of community trust in the Census has been impacted by:
    - The announcement prior to the 2016 Census that names and addresses would be retained;
    - The decision not to complete an independent PIA prior to that decision;
    - Limitations in the public consultation on that decision; and
    - Issues related to the online process for the 2016 Census;
- Although considerable public information is available regarding the 2021 Census (e.g. on the ABS website), this information does not (yet) address or discuss some of the key privacy issues that are likely to be of interest to individuals;
- The 2021 Census has not (yet) been the subject of a full independent security risk assessment;
- The implementation of the 2021 Census is heavily reliant on partners, third party service providers, outsourcing, cloud services and third party apps;
- Significant amounts of personal information, including sensitive personal information, are collected from third parties;
- 2021 Census data will be combined with other datasets as part of the Multi-Agency Data Integration Project (MADIP);
- Some concerns have been raised regarding the ability of ABS (and similar organisations) to effectively de-identify data when it is released to researchers;
- New questions, including questions on military service and long-term health conditions (including a mental health condition response option), have been included in the 2021 Census, with minimal engagement with key privacy stakeholders;
- The 2021 Census privacy protections face a potential risk of being over-ridden by the proposed Data Availability and Transparency legislation (the proposed DATA Framework); and
- 2021 Census data is subject to complex, inconsistent and lengthy data retention periods.

5. Structural Privacy Recommendations

This PIA includes three major Structural Recommendations. These are key mechanisms to ensure a lasting, layered and sustainable Privacy by Design approach is adopted for the Census (for 2021 and beyond).

Structural Recommendation 1: Census Privacy Strategy

The ABS should develop and implement a 7-8 year Census Privacy Strategy that covers more than one Census.

During the PIA process and stakeholder consultations it emerged that some privacy issues and concerns related to the Census may be exacerbated by the 'one-off' approach to Census privacy management. That is, the Census is only conducted every five years and some aspects of the Census, including some privacy aspects, are managed as stand-alone project management issues. For example, the development of the content of the Census, including ABS consultation on the Census questions, occurred prior to the commencement of the PIA.

Also, during the PIA process it became apparent that some potential privacy protection measures may take a long time to be refined and implemented, with the benefits only being realised well after completion of the 2021 Census. Rather than abandoning these measures, Galexia is recommending including them in a longer-term Census Privacy Strategy so that they can be implemented for future Censuses.

In developing this Recommendation, Galexia suggests that the Census Privacy Strategy should cover a period of 7-8 years, so that it straddles two Census periods.

The contents of the Census Privacy Strategy should include:

- Integration of multiple PIAs (e.g. Census PIAs would be cumulative and reflect on the implementation of Recommendations in earlier PIAs, as well as addressing new issues);
- Integration of the PIA with the development of Census content, to ensure that privacy issues are addressed during the development and approval of new Census topics and questions;
- Integration of key stakeholder consultation on Census privacy issues, so that there are no longer two separate processes for talking to key privacy stakeholders (on content and on the PIA); and
- Inclusion of long-term privacy objectives and targets.

Currently there is no long-term Census Privacy Strategy in place, and this makes it difficult to set privacy targets and establish appropriate governance mechanisms to ensure these targets are met. There is a risk that a stand-alone PIA will need to rush through more restrictive recommendations to protect privacy in the absence of a long-term strategy.

This PIA suggests the following privacy targets should be included in the proposed Census Privacy Strategy:

Galexia Proposed Privacy Targets for a long-term Census Privacy Strategy		
	Privacy Target	**Governance**
1	**The amount of sensitive data collected in the Census should be reduced in accordance with the data minimisation principle.**	Each Census PIA should assess Census questions and report on efforts to minimise the collection of sensitive data. Over time, the amount of sensitive data collected should be reduced, not expanded.
2	**Census questions should not be stigmatising, intrusive or capable of triggering a trauma response in individuals.**	The ABS should continue to ensure that Census questions and language reflect contemporary approaches to reducing stigma and managing intrusion and trauma for some individuals. Questions and language that might work in other settings (e.g. a specific field survey) may not be appropriate in the Census.
3	**ABS legislation should be expanded to include a list of permitted and prohibited purposes for the use of Census data.**	A long-term goal for the Census should be to enhance privacy protections in ABS legislation, including specific sets of permitted and prohibited purposes for the use of Census data. Such reforms are likely to take some time to build consensus, develop and implement. Although they would not be in place for the 2021 Census, they could be ready for the following Census.
4	**Reduce data retention periods for identifying information (e.g. name and address).**	The Census Privacy Strategy should include a phased reduction in data retention periods for identifying data, in order to better manage privacy risks, and more closely match specific business needs. The Census Privacy Strategy and each PIA should ensure there is downward pressure on data retention periods.
5	**Reform the refusals and prosecution process to implement a better balance between response rates and consequences for individuals facing prosecution.**	The Census Privacy Strategy should include a review of the refusals and prosecution process for non-completion of the Census, including the Referral for Prosecution Policy and maximum penalty provisions.

During the PIA process the proposed Census Privacy Strategy and the suggested privacy targets have received support from key stakeholders. A major concern raised by stakeholders in relation to both the 2016 Census and leadup to the 2021 Census was a lack of engagement on key policy decisions regarding name retention and new Census content.

For example, many key stakeholders had not seen the proposed new topics and questions for the 2021 Census until they were presented during PIA stakeholder workshops in October and November 2019. By this date, the main consultation on the new ABS topics and questions was closed. A further short consultation was conducted by the Treasury in December 2019. However, this consultation was conducted over the Christmas break and was very low profile. The actual wording of the proposed questions was not provided as part of this short consultation. Submissions were not made public and the proposed new topics and questions were approved without detailed reference to privacy issues. Refer to Appendix F – Consultation Timeline on 2021 Census Topics.

The proposed Census Privacy Strategy should help to avoid this situation arising again, and ensure a closer level of ongoing engagement between privacy issues and the content of future Censuses, as well as incorporating more meaningful opportunities for stakeholder input.

Structural Recommendation 2: Principles based approach to name encoding for data linkage

The ABS should develop and implement a principles based approach to the issue of name encoding for data linkage.

Name encoding is one of the key processes used by the ABS to link Census data with other datasets. During the PIA process it has become apparent that this process is the subject of considerable concern amongst external stakeholders, and that the process is poorly understood outside the ABS.

Galexia rates this issue as one of the most significant risks for the Census, due to the widespread perception that Census data is being added to a large and ongoing national dataset, that is easily linked to named individuals.

Galexia considered two options for managing this issue:

- **Option 1: Endorse a specific technical approach**
  Under Option 1, this PIA could make an assessment of the specific technology proposed by the ABS for the Census. For example, the ABS is proposing to use a form of Lossy encoding[21] for the 2021 Census. If satisfied with the privacy protection offered by this technology, the PIA could endorse that approach. However, there is a risk that a specific technology may become outdated or shown to be vulnerable at any time, and each Census PIA would need to revisit the issue in detail and examine (and potentially endorse) a new technical approach.
- **Option 2: Adopt a principles based approach**
  Under Option 2, this PIA could set out a suggested principles based approach to managing this issue, which could be used by the ABS on an ongoing basis. This approach would give confidence to stakeholders that the issue was the subject of regular review and oversight.

After discussion with ABS and key stakeholders, Galexia recommends the development of a principles based approach (Option 2) to managing name encoding for data linkage, including the following features:

1) Raw name data should not be used;
2) Any linkage key that is retained should not be reversible to a name;
3) It is not necessary for linkage to be 100% accurate and the ABS should be transparent about accuracy rates;
4) The ABS should provide reasonable transparency regarding the name encoding process and the linkage methodology, although some reasonable caution regarding specific details is permissible;
5) The name encoding approach should not be fixed – it should be subject to regular reviews;
6) The ABS must establish an appropriate process for engaging with stakeholders, critics and external experts regarding the name encoding process; and
7) An exceptions provision should be included to allow alternative methodologies for name linking in exceptional circumstances where a linking project demonstrates a clear public benefit and does not raise the overall risk profile for Census data (for example, refer to the project: Linking Death registrations to the 2016 Census[22]).

[21] ABS, *Information paper: Name encoding method for Census 2016* (6 March 2018) <www.abs.gov.au/websitedbs/d3310114.nsf/home/Information+paper+Name+encoding+method+for+Census+2016>

ABS, *1351.0.55.162 – Research Paper: Options for Encoding Name Information for use in Record Linkage* (2018) <www.abs.gov.au/ausstats/abs@.nsf/mf/1351.0.55.162>

[22] ABS, *3302.0.55.004 – Linking Death registrations to the 2016 Census* (2016-17) <www.abs.gov.au/ausstats/abs@.nsf/mf/3302.0.55.004>

During the PIA process some stakeholders expressed a preference for a specific technical approach to name encoding and linking (e.g. some academic experts on linking technologies). However, Galexia considers that it is reasonable for the ABS to adopt a principled approach, and we do not endorse any single technical approach.

Some privacy advocates accept the recommended approach, but query whether names should be collected at all in the Census. In practice, names play a vital role in reconciliation as well as linking. For example, an individual may complete their own personal form, but their information may also be included by a third party on a household form. Names are used to ensure that the two records are reconciled and only counted once. This is just one example of the vital role that names play in ensuring the quality of Census data.

Overall, there was support for the suggested principles based approach from key stakeholders, including privacy regulators and some advocacy groups.

Structural Recommendation 3: Principles based approach to managing re-identification risk

The ABS should develop and implement a principles based approach to managing re-identification risk.

During the PIA process it has become apparent that re-identification risk is the subject of considerable concern amongst external stakeholders. Some key stakeholders (including regulators) have no confidence that re-identification can be prevented where any form of detailed data is released. Other stakeholders have raised specific issues with current ABS de-identification processes. Concerns about this issue have been amplified for the 2021 Census by the proposed inclusion of a new question on long-term health conditions that may make some individuals easier to re-identify.

Galexia considers this issue as one of the most significant risks for the Census, due to the strength and consistency of stakeholder concerns regarding re-identification risk.

Galexia has considered two options for managing this issue:

- **Option 1: Endorsing a specific technical approach**
  Under Option 1, the PIA would make an assessment on the specific technology proposed by the ABS for the 2021 Census (currently a customised, layered approach to removing or obscuring data depending on the chosen output, complemented by other privacy and security protection measures such as vetting and monitoring). If satisfied with the privacy protection offered by this approach, the PIA would need to endorse that specific technical approach. However, there is a risk that a specific technology may become outdated or shown to be vulnerable at any time, and each Census PIA would need to revisit the issue in detail and examine (and potentially endorse) a new technical approach.
- **Option 2: Adopting a principles based approach**
  Under Option 2, the PIA will set out a suggested principles based approach to managing this issue, which can be used by the ABS on an ongoing basis. This approach would give confidence to stakeholders that the issue was the subject of regular review and oversight.

Galexia recommends adopting a principles based approach (Option 2) to managing re-identification risk, including the following features:

1) The ABS should continue to employ a layered approach to managing re-identification risk, so that it is not relying too heavily on one single protection measure;
2) Strict vetting processes should be in place for access to all but the lowest risk data;

3) Researchers and third parties should be bound by legal agreements to not attempt re-identification without ABS permission and oversight;
4) Researchers and third parties should be bound by legal agreements to not release any outputs that might identify individuals;
5) The ABS should have full technical capacity to monitor all access, including individual research queries and patterns of queries;
6) The ABS should have full technical capacity to throttle queries and / or suspend and revoke access;
7) The ABS should adopt sound approaches to removing, obscuring or perturbing data, although the PIA is not suggesting that this approach should be at the cost of reasonable utility;
8) The ABS should provide reasonable transparency regarding the process for managing re-identification risk, although some caution regarding revealing specific details is permissible;
9) The technical approach to de-identification should not be fixed – it should be subject to a formal annual review;
10) The ABS must establish an appropriate process for engaging with stakeholders, critics and external experts regarding the de-identification process; and
11) An exceptions provision should be included to allow alternative methodologies for managing re-identification risk in exceptional circumstances.

During the PIA process some stakeholders expressed a preference for a specific technical approach to managing de-identification. However, Galexia considers that it is reasonable for the ABS to adopt a layered approach to managing this risk, in an attempt to strike a balance between privacy and utility. The approach is similar to the 'security in depth' approach, where an organisation attempts to avoid relying on a single protection measure.

Although the ABS has been following this approach for some time, it would benefit from improved documentation, a more formal approach to engaging with stakeholders, and enhanced oversight and review. A principles based approach should help the ABS to achieve these aims.

Australian Privacy Principles (APPs) and the 2021 Census

6. Classification of Data – Is the Data 'personal information' or 'sensitive information'?

6.1. The Law

A starting point for our discussion of privacy compliance is whether or not the 2021 Census data is personal information.

The *Privacy Act 1988* (Cth) states:

> *Personal information means information or an opinion about an identified individual, or an individual who is reasonably identifiable.*
> <www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-b-key-concepts/#personal-information>

6.2. OAIC Guidance

In May 2017 the OAIC provided guidance on personal information:

> *What Is Personal Information?,* Office of the Australian Information Commissioner (OAIC), 5 May 2017 <www.oaic.gov.au/privacy/guidance-and-advice/what-is-personal-information>.

The Privacy Commissioner warns that:

> *where it is unclear whether an individual is 'reasonably identifiable', an organisation should err on the side of caution and treat the information as personal information.*[23]

6.3. Census – Overview

The 2021 Census will incorporate questions requiring a mix of personal information and sensitive personal information.

For the 2021 Census, nearly all of the data that is being collected will be linked to an individual, or can be linked to the correct individual. After collection there are questions about whether the data *remains* personal information, as names are removed and other steps are taken to de-identify data once it is used in statistical publications or data integration projects. This issue is discussed in more detail throughout the PIA.

An additional question is whether or not some of the data falls into the category of sensitive information.

Sensitive information[24] means:

> *(a) information or an opinion about an individual's:*
>
> *(i) racial or ethnic origin; or*
> *(ii) political opinions; or*
> *(iii) membership of a political association; or*
> *(iv) religious beliefs or affiliations; or*
> *(v) philosophical beliefs; or*
> *(vi) membership of a professional or trade association; or*
> *(vii) membership of a trade union; or*
> *(viii) sexual orientation or practices; or*
> *(ix) criminal record;*
> *that is also personal information; or*
>
> *(b) health information about an individual; or*

[23] Office of the Australian Information Commissioner (OAIC), *Guide to securing personal information*, 2015, <www.oaic.gov.au/privacy/guidance-and-advice/guide-to-securing-personal-information>.

[24] Section 6 of the *Privacy Act 1988 (Cth)* <www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/s6.html>.

(c) genetic information about an individual that is not otherwise health information; or

(d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or

(e) biometric templates.

The table below summarises some of the key data fields collected during the Census:[25]

Data category	Main Sources	Personal information?	Sensitive personal information?
Name	• Census form • Field contact • Contact centre communication	**Yes**	
Basic demographic details (age, marital status etc.)	• Census form	**Yes**	
Address	• Census form • Field contact • Contact centre communication • Correspondence	**Yes**	
Other contact details (phone, email)	• Field contact • Contact centre communication • Correspondence	**Yes**	
Racial and ethnic origin	• Census form	**Yes**	**Yes**
Religion	• Census form (optional)	**Yes**	**Yes**
Employment and financial details	• Census form • Third parties	**Yes**	
Health information	• Census form	**Yes**	**Yes**
Criminal record	• Third parties • (implied by location)	**Yes**	**Yes**
Education level attained	• Census form	**Yes**	
Defence Force service	• Census form	**Yes**	
Census Number	• Census form • Field work	**Yes**	

6.4. 'Personal information' Finding

The 2021 Census will incorporate questions requiring a mix of personal information and sensitive personal information.

The presence of sensitive information has implications for APP 3 and APP 6 (discussed below). It also raises the overall security profile of the proposal (discussed in APP 11 below).

[25] More detailed information on data fields is outlined in Appendix C – ABS 2021 Census contact points with the public and the 2021 Census Privacy Statement (available at <www.census.abs.gov.au/privacy> from mid-October 2020).

7. APP 1. Open and Transparent Management of Personal Information

7.1. APP 1. The Law

APP 1 — open and transparent management of personal information

1.2 An APP entity must take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to the entity's functions or activities that:

> *(a) will ensure that the entity complies with the APPs / registered code; and*
>
> *(b) will enable the entity to deal with inquiries or complaints from individuals about the entity's compliance with the APPs / registered code.*

1.3 An APP entity must have a clearly expressed and up to date policy (the APP privacy policy) about the management of personal information by the entity.

1.4 (minimum contents of the privacy policy)

1.5 An APP entity must take such steps as are reasonable in the circumstances to make its APP privacy policy available:

> *(a) free of charge; and*
>
> *(b) in such form as is appropriate.*

More information: <www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-1-app-1-open-and-transparent-management-of-personal-information>.

7.2. APP 1. 2021 Census – Overview

ABS has previously maintained a public Privacy Policy and a specific Census Privacy Policy.[26] The privacy policies are complemented by other online and offline privacy information resources, including brochures and 'privacy scripts' that are used in the Contact Centre.

During the course of this PIA the ABS and Census Privacy Policies have been under review, and Galexia has provided early advice to the ABS on how these policies could be enhanced / improved.

Some of this history is summarised briefly in the following table:

APP 1. Privacy policy issues resolved	Earlier Galexia advice	Action taken by ABS
A. The existing policies did not accurately reflect the amount of data that is likely to be collected from third parties in the 2021 Census.	Galexia provided advice to the ABS that recommended amending an example used in the draft privacy policy and expanding the description of third party collection.	The current draft of the Census privacy notice[27] states: *One person in the household or dwelling usually completes the form for everyone at home on Census night. If you are living in a group house, or want to keep your information private from others in your household, go to www.census.abs.gov.au.[28] A range of different self-service options are available to help you complete your Census form.*

[26] For example:

- *Main ABS Privacy Policy* <www.abs.gov.au/websitedbs/D3310114.nsf/Home/Privacy+Policy>
- *2016 Census Privacy Policy* <www.abs.gov.au/websitedbs/censushome.nsf/home/privacypolicy>

[27] ABS, *Collection of your personal information in the 2021 Census of Population and Housing* (24 April 2020) [internal working document]

[28] Note: this link will be available from mid-October 2020.

		It is expected that the new ABS Privacy Policy will follow this approach.
B. The existing Census Privacy Policy did not clearly set out all of the potential 'paths' for personal information once it was collected.	Galexia provided advice to the ABS that recommended listing all four potential data pathways.	The current draft of the Census privacy notice now lists all four data paths: 1) Core Census activities (all data); 2) Data Integration (all data); 3) Time Capsule (consent based, about 50% of data); and 4) Longitudinal study (5% of data). It is expected that the new ABS Privacy Policy will follow this approach.
C. The existing ABS and Census privacy policies did not have working / accurate links to formal data retention policies (Records Authorities) and some relevant links at the National Archives were also not working.	Galexia provided advice to the ABS that noted inaccurate and broken links.	The ABS Privacy Policy[29] now includes accurate / working links to the correct Records Authorities. Links at the National Archives have also been corrected.

In addition, this PIA has been considering whether or not the ABS should continue to use a separate privacy policy for the Census. During the course of this PIA, the ABS has decided to draft a general ABS Privacy Policy that covers all ABS activities, supplemented by separate pages with more details on specific collections and activities (such as MADIP and the Census) and as of April 2020 this is being actively reviewed and updated by ABS.

Galexia's view is that this will only work if each Census Privacy Policy sub-section or appendix is clearly dated and an archive of prior policies is maintained. For example, consumers should be able to easily find the specific privacy policy that applied to a particular Census (2016 and 2021 at least). This is because each Census has different privacy rules on key issues such as data retention periods.

The following table summarises compliance with APP 1:

APP 1. Open and transparent management of personal information	Action / Status	Galexia Commentary
A. Does the entity provide a public privacy policy?	**Action required**	As of April 2020, the ABS is drafting a new overarching privacy policy to cover all of its activities. During the development of this PIA, Galexia has provided input on key issues that have now been addressed in the new draft policy (Refer to the APP 1. Privacy policy issues resolved above). One outstanding issue is the question of whether there should be a stand-alone Census Privacy Policy. This PIA recommends that the privacy policy (whether it is a generic ABS Privacy Policy or a stand-alone Census Privacy Policy) should have a clear, separate section covering the specific features of each Census. This is because the content and the data retention periods change for each Census. **Recommendation 1: Develop and maintain separate Census Privacy Policy sections** Each Census Privacy Policy sub-section or appendix should be clearly dated and an archive of prior policies should be maintained (for the 2016 and 2021 Censuses at least).

[29] ABS, *Privacy Policy* (6 January 2020) <www.abs.gov.au/websitedbs/D3310114.nsf/Home/Privacy+Policy>

B. Does the Policy include: (a) the kinds of personal information that the entity collects and holds;	**Compliant**	The draft policy lists the general categories of data that are collected and held by the ABS in the Census. The Census form is also an excellent source of information on the categories of data collected.
C. Does the Policy include: (b) how the entity collects and holds personal information;	**Compliant**	The draft policy lists the general methods of data collection used by the ABS.
D. Does the Policy include: (c) the purposes for which the entity collects, holds, uses and discloses personal information;	**Compliant**	The draft policy lists the general purposes of data collection for the Census. The Census form is also an excellent source of information on the use of data. For example, the online Census form allows users to read further information about how the ABS uses specific data. The paper form provides a free call number for users with specific queries, with web references against questions where more explanation of the topic is required.
E. Does the Policy include: (d) how an individual may access personal information about the individual that is held by the entity and seek the correction of such information;	**Compliant** **Further measures possible**	The draft policy includes information on access requests. **Note**: This is an area where there is room for some improvement – Refer to Recommendation 7: Clarify access rules for different categories of data in APP 12 below.
F. Does the Policy include: (e) how an individual may complain about a breach of the APPs / registered code, and how the entity will deal with such a complaint;	**Compliant**	The draft policy includes information on complaints.
G. Does the Policy include: (f) whether the entity is likely to disclose personal information to overseas recipients;	**Compliant**	The draft Census privacy notice[30] explains that information from the Census is not transferred overseas. It states: *Personal information is not shared or disclosed to overseas parties.* *Personal information in the cloud is kept in Australia.* This wording will be used in the proposed Census Privacy Policy section.
H. Does the Policy include: (g) if the entity is likely to disclose personal information to overseas recipients—the countries in which such recipients are likely to be located if it is practicable to specify those countries in the policy.	**Compliant**	n/a

7.3. APP 1. Finding

Overall, this PIA has found that the compliance status for APP 1 is: Action required.

[30] ABS, *Collection of your personal information in the 2021 Census of Population and Housing* (24 April 2020) [internal working document]

8. APP 2. Anonymity and Pseudonymity

8.1. APP 2. The Law

APP 2 — anonymity and pseudonymity

2.1 Individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with an APP entity in relation to a particular matter.

2.2 Subclause 2.1 does not apply if, in relation to that matter:

> *(a) the APP entity is required or authorised by or under an Australian law, or a court/tribunal order, to deal with individuals who have identified themselves; or*
>
> *(b) it is impracticable for the APP entity to deal with individuals who have not identified themselves or who have used a pseudonym.*

More information: <www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-2-app-2-anonymity-and-pseudonymity>.

8.2. APP 2. 2021 Census – Overview

The following table summarises compliance with APP 2:

APP 2. Anonymity	Action / Status	Galexia Commentary
A. Where lawful and practicable, are individuals given the option of: – Not identifying themselves?	**Compliant**	The ABS provides anonymity to users in appropriate circumstances – for example general web site visitors can access information about the Census without providing personal information. All other data collected via the 2021 Census is covered by exceptions to the anonymity principle. For example, the ABS is authorised to collect names on Census forms so that they can reconcile records where an individual appears on more than one form (e.g. an individual form and a household form completed by a third party).
B. Where lawful and practicable, are individuals given the option of: – Identifying themselves with a pseudonym?	**Compliant**	The ABS does not provide a pseudonymous option directly to consumers. However, in practice, Census data is de-identified before it is used in publications and data products made available to researchers, and this serves a similar role to a pseudonym.

8.3. APP 2. Finding

Overall, this PIA has found that the compliance status for APP 2 is: Compliant.

9. APP 3. Collection of Solicited Personal Information

9.1. APP 3. The Law

APP 3 — collection of solicited personal information

Personal information other than sensitive information

3.1 If an APP entity is an agency, the entity must not collect personal information (other than sensitive information) unless the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities.

3.2 If an APP entity is an organisation, the entity must not collect personal information (other than sensitive information) unless the information is reasonably necessary for one or more of the entity's functions or activities.

Sensitive information

3.3 An APP entity must not collect sensitive information about an individual unless:

(a) the individual consents to the collection of the information and:

(i) if the entity is an agency — the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities; or

(ii) if the entity is an organisation — the information is reasonably necessary for one or more of the entity's functions or activities; or

(b) subclause 3.4 applies in relation to the information.

3.4 This subclause applies in relation to sensitive information about an individual if:

(a) the collection of the information is required or authorised by or under an Australian law or a court/tribunal order; or

... [Note: some further exceptions are available]

3.5 An APP entity must collect personal information only by lawful and fair means.

3.6 An APP entity must collect personal information about an individual only from the individual unless:

(a) if the entity is an agency:

(i) the individual consents to the collection of the information from someone other than the individual; or

(ii) the entity is required or authorised by or under an Australian law, or a court/tribunal order, to collect the information from someone other than the individual; or

(b) it is unreasonable or impracticable to do so.

Some additional exceptions known as permitted general situations also apply – these can be found in Section 16A of the Act.

9.2. APP 3. OAIC Guidelines

APP 3 sets out the requirements for the collection of personal information. The Office of the Australian Information Commissioner (OAIC) has issued guidelines on APP 3 that warn there are privacy risks associated with:

- Collecting personal information about a group of individuals, when information is only required for some of those individuals;
- Collecting more personal information than is required for a function or activity; or

- Collecting personal information that is not required for a function or activity but is being entered in a database in case it might be needed in the future.

In addition to these risks, the collection of personal information should generally be kept to a minimum and personal information should normally be collected from the data subject.

More information: <www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-3-app-3-collection-of-solicited-personal-information>.

9.3. APP 3. 2021 Census – Overview

This PIA is being completed after the finalisation of the Census topics and questions, so consideration of the content of the Census questions during the PIA process has been limited. This has been the cause of significant concern amongst external stakeholders, who believe that the inclusion of two new Census topics (on veterans and long-term health conditions) raised serious privacy issues. Please note that the issues around the process for adding new topics and questions to the Census are discussed in Structural Recommendation 1: Census Privacy Strategy, rather than here in the discussion of APP 3.

The following table summarises compliance with APP 3:

APP 3. Collection of solicited information	Action / Status	Galexia Commentary
A. Is collected information reasonably necessary for, or directly related to, one or more of the entity's functions or activities?	**Compliant**	The data minimisation test in APP 3.1. applies even where the collection of data is required or authorised by legislation. The data minimisation requirement applies to both the initial collection of data from consumers, and the subsequent use of data in data integration projects. This is because the sharing of data with a third party (e.g. in a data integration project) results in a new 'collection' by that third party. The ABS does apply a data minimisation approach to the selection of topics and questions for the Census, and a separate data minimisation test applies to the collection and use of personal information in data integration programs. It is important to note that many stakeholders raised concerns that the new health question to be included in the 2021 Census was an unreasonable intrusion into the privacy of individuals, and they did not believe it was justified. In their view it represents a breach of the data minimisation principle in APP 3. The health question asks for information on long-term health conditions (including a mental health condition response option). The exact wording of the health question is yet to be confirmed, but it is likely to be the same as the text used in the Census Test Form (October 2019) and is extracted in Appendix B – Extracts from the Census Test Forms. This PIA is unable to re-open consideration of the inclusion of the health question in the 2021 Census. However, we do make several recommendations to strengthen other privacy and security safeguards in recognition of the added risks of including sensitive health data in the Census (for example Recommendation 5: Shorten data retention periods for names and Recommendation 15: Remove the new health data collected in the 2021 Census from data submitted to the Time Capsule) The issue of the process for adding new Census questions is discussed above in Structural Recommendation 1.

B. Is NO sensitive information about an individual collected (unless a relevant exception applies, such as the receipt of explicit and specific consent)?	**Compliant**	Significant amounts of sensitive information are collected in the Census. Categories (based on the *Privacy Act* definition of Sensitive Information) include: • **Racial or ethnic origin** – the Census contains numerous detailed questions on race. Some additional data may also be recorded during field work (e.g. where a field officer visits a remote Indigenous community); • **Religious beliefs or affiliations** – the Census contains a single, optional question on religion; • **Sexual orientation or practices** – there is no direct question in the Census but the category might be imputed by reference to other data (e.g. a person living with a same sex partner). Data quality for this approach is low as it only captures persons who normally live together; • **Criminal record** – there is no direct question in the Census, but the category might be imputed by location (e.g. correctional facility); and • **Health information** – the Census contains a new question on long-term health conditions and there are some existing questions on care and assistance requirements which are likely to reveal health information. Compliance with APP 3 in relation to sensitive information is managed by relying on the authorised by law exception (as the Census / ABS legislation authorises the collection of this data). The collection of data on religious beliefs is also based on consent, as this question is the only question in the Census marked as 'optional'.
C. Is personal information collected only by lawful and fair means?	**Compliant**	All information is collected by lawful and fair means.
D. Is personal information about an individual collected only from the individual (unless a relevant exception applies)?	**Compliant** **Further measures possible**	APP 3 requires entities to limit the collection of data from third parties. A significant amount of data is collected from third parties in the Census. Although this is done in compliance with the ABS legislation and the *Privacy Act,* more could be done to encourage the use of individual forms. This is an important issue for the 2021 Census because the form now requires the collection of additional sensitive information (such as questions regarding long-term health conditions with one response option including mental health conditions). In the 2016 Census only a very small number of requests were received for individual forms (fewer than 100,000). This may include some households that requested an extra form because there were more than six people in the household (the paper form only had six columns). **Recommendation 2: Promote alternatives to third party collection** The ABS should explore measures to address the extent of third party collection of data. For example, more could be done to promote the option to use individual paper and online forms. Note: At the time of completing this PIA a 2021 Census privacy notice[31] has been drafted which provides the following advice: ***How is your personal information collected?*** *From the Census form, which you can complete online or on a paper form. One person in the household or dwelling usually completes the form for everyone at home on Census night. If you are living in a group house, or wish to keep your information private from others in your household, go to www.census.abs.gov.au.[32] A range of different self-service options are available to help you complete your Census form.*

[31] ABS, *Collection of your personal information in the 2021 Census of Population and Housing* (24 April 2020) [internal working document]

[32] Note: this link will be available from mid-October 2020.

		The ABS has also advised that they plan to add specific wording to the online form – reminding the head of the household that individual forms should be offered to household members if they prefer. Similar wording will be added to the paper form.

9.4. APP 3. Finding

Overall, this PIA has found that the compliance status for APP 3 is: Compliant (further measures possible).

10. APP 4. Dealing with Unsolicited Personal Information

10.1. APP 4. The Law

APP 4 provides that organisations that receive unsolicited personal information are required to determine whether or not they could have collected the information under APP 3. If they determine that they could **not** have collected the personal information, the information must be destroyed.

More information: <www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-4-app-4-dealing-with-unsolicited-personal-information>.

10.2. APP 4. 2021 Census – Overview

It is impossible to rule out the receipt of unsolicited information by the ABS. APP 4 requires agencies and organisations to assess unsolicited information as it arrives, and destroy it if it is information that they could not have collected themselves.

The following table summarise compliance with APP 4:

APP 4. Dealing with unsolicited information	Action / Status	Galexia Commentary
A. Are there circumstances in which the ABS may receive unsolicited personal information?	**Compliant**	Some unsolicited personal information may be provided, particularly during field work.
B. Does the ABS have a policy in place for managing unsolicited personal information in accordance with the *Privacy Act*?	**Compliant**	The ABS privacy training includes coverage of this issue. The ABS has appropriate measures in place to handle the receipt of unsolicited information.

10.3. APP 4. Finding

Overall, this PIA has found that the compliance status for APP 4 is: Compliant.

11. APP 5. Notification of the Collection of Personal Information

11.1. APP 5. The Law

APP 5 — notification of the collection of personal information

5.1 At or before the time or, if that is not practicable, as soon as practicable after, an APP entity collects personal information about an individual, the entity must take such steps (if any) as are reasonable in the circumstances:

> *(a) to notify the individual of such matters referred to in subclause 5.2 as are reasonable in the circumstances; or*
>
> *(b) to otherwise ensure that the individual is aware of any such matters.*

5.2 The matters for the purposes of subclause 5.1 are as follows:

> *(a) the identity and contact details of the APP entity;*
>
> *(b) if:*
>
> > *(i) the APP entity collects the personal information from someone other than the individual; or*
> >
> > *(ii) the individual may not be aware that the APP entity has collected the personal information;*
>
> *the fact that the entity so collects, or has collected, the information and the circumstances of that collection;*
>
> *(c) if the collection of the personal information is required or authorised by or under an Australian law or a court/tribunal order — the fact that the collection is so required or authorised (including the name of the Australian law, or details of the court/tribunal order, that requires or authorises the collection);*
>
> *(d) the purposes for which the APP entity collects the personal information;*
>
> *(e) the main consequences (if any) for the individual if all or some of the personal information is not collected by the APP entity;*
>
> *(f) any other APP entity, body or person, or the types of any other APP entities, bodies or persons, to which the APP entity usually discloses personal information of the kind collected by the entity;*
>
> *(g) that the APP privacy policy of the APP entity contains information about how the individual may access the personal information about the individual that is held by the entity and seek the correction of such information;*
>
> *(h) that the APP privacy policy of the APP entity contains information about how the individual may complain about a breach of the Australian Privacy Principles, or a registered APP code (if any) that binds the entity, and how the entity will deal with such a complaint;*
>
> *(i) whether the APP entity is likely to disclose the personal information to overseas recipients;*
>
> *(j) if the APP entity is likely to disclose the personal information to overseas recipients — the countries in which such recipients are likely to be located if it is practicable to specify those countries in the notification or to otherwise make the individual aware of them.*

More information: <www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-5-app-5-notification-of-the-collection-of-personal-information>.

11.2. APP 5. 2021 Census – Overview

During the course of this PIA the Census forms and privacy notices have been under review, and Galexia has provided early advice to the ABS on how these forms and notices could be enhanced / improved.

Some of this history is summarised briefly in the following table:

APP 5. Notification issues resolved	Earlier Galexia advice	Action taken by ABS
A. Census privacy notices were scattered across multiple ABS contact points and were sometimes inconsistent.	The EY pre-PIA Review[33] recommended that every contact point should be examined (for compliance with APP 5 and also for consistency). Galexia provided advice to the ABS to improve the consistency of key privacy messages across all Census contact points and privacy notices.	The ABS has created a comprehensive table of contact points with the public for the Census collection (Refer to Appendix C – ABS Contact points with the public) and also for Census employees. The ABS is committed to ensuring consistency of key privacy messages across all communication channels.
B. The ABS did not use standard wording to explain the four potential data pathways for Census data	Galexia provided advice to the ABS that recommended the development of standard wording to describe the four data pathways for Census data.	The current draft of the Census privacy notice[34] now clearly summarises the four data pathways: • ***Core statistics*** *– these help inform administration, policy development and planning activities of governments, businesses, communities, researchers and other users.* • ***Data integration*** *– this is where Census information is combined with data from other sources to create new and more valuable statistics. For more information see the data integration[35] page on the ABS website. Information about you is not identifiable from this process, or in the new statistics.* • ***Australian Census Longitudinal Dataset*** *– this uses a 5% sample of data from the three most recent Censuses (2006-2016). This 5% sample will be combined with corresponding 2021 Census data to build a picture of how Australian society is changing over time.* • ***Census Time Capsule*** *– you can decide to have your Census information transferred to the National Archives. If you choose to have this done, your information will not be made available for any purpose until 2120. It cannot be accessed for any reason before that time. You can read about the Census Time Capsule on our website.[36]*

[33] EY, Pre-PIA Review, Census 2021 (11 September 2019) [internal document]

[34] ABS, *Collection of your personal information in the 2021 Census of Population and Housing* (24 April 2020) [internal working document]

[35] <www.abs.gov.au/websitedbs/D3310114.nsf/Home/Statistical+Data+Integration>

[36] <www.abs.gov.au/ausstats/abs@.nsf/Lookup/by%20Subject/2008.0~2016~Main%20Features~Census%20Time%20Capsule~143>

C. The ABS did not use standard wording to explain the extent of third party data collection in the Census	Galexia provided advice to the ABS that recommended the development of standard wording to describe third party data collection in the Census.	The current draft of the Census privacy notice states: *One person in the household or dwelling usually completes the form for everyone at home on Census night. If you are living in a group house, or want to keep your information private from others in your household, go to www.census.abs.gov.au.*[37] *A range of different self-service options are available to help you complete your Census form.*

The process for providing Census privacy notices to consumers is complex, as the Census has multiple 'contact points' with members of the public. A detailed table of all contact points is provided at Appendix C – ABS Contact points with the public.

Some of the key information flows are also summarised in the following diagram:

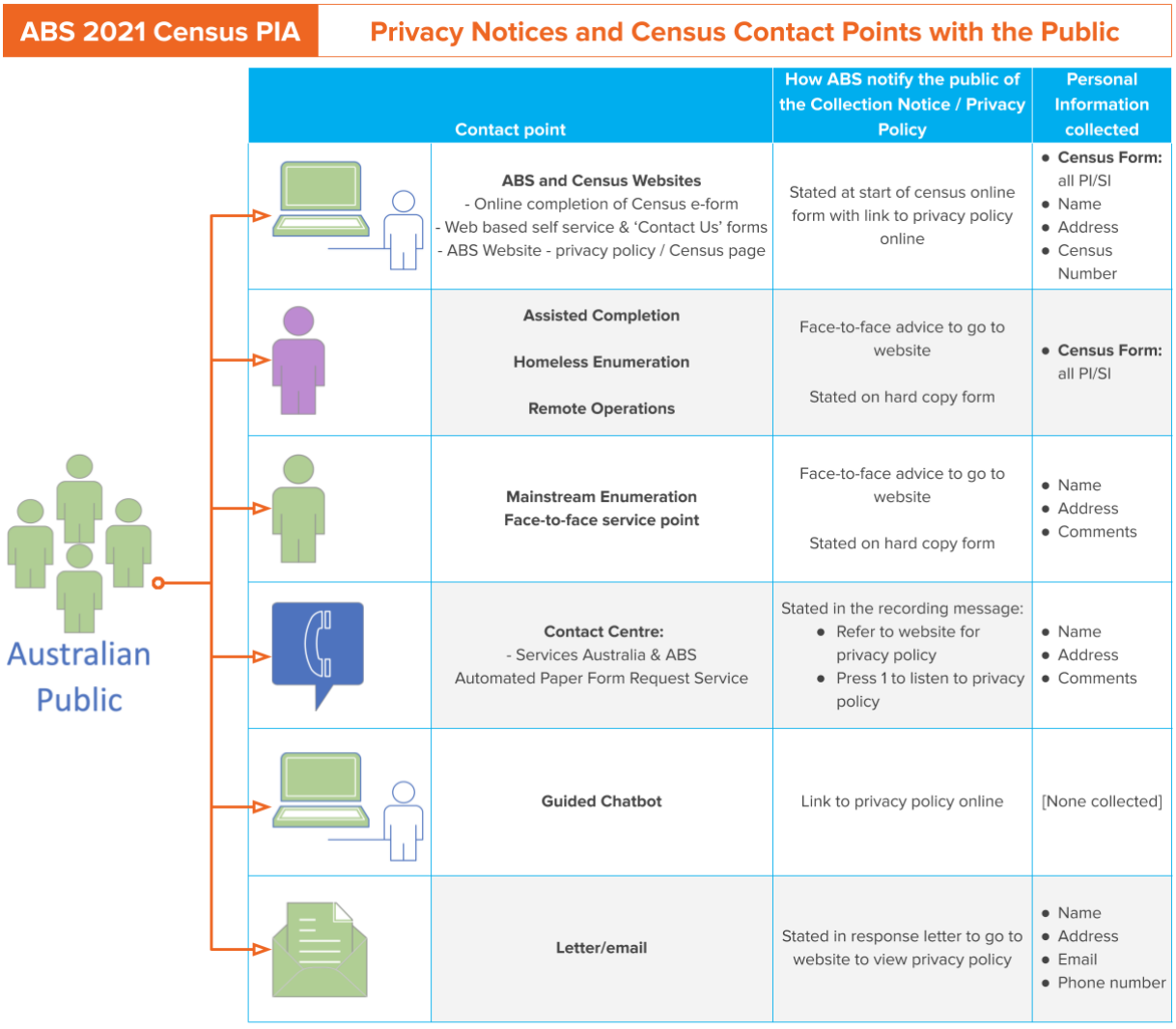


Diagram: 2021 Census contact points (information supplied by ABS – April 2020)

The following table summarises key tasks for the ABS to ensure compliance with APP 5 for the 2021 Census:

[37] Note: this link will be available from mid-October 2020.

APP 5. Notification	Action / Status	Commentary
A. Does the entity provide notice of its identity and contact details?	**Compliant**	The Census privacy notice and the Census form both provide clear identity and contact details.
B. Does the entity provide notice of third party collection? (if relevant)	**Compliant**	At the time of completing this PIA a Census privacy collection notice has been drafted which provides the following advice: ***How is your personal information collected?*** *From the Census form, which you can complete online, or via a paper form. One person in the household or dwelling usually completes the form for everyone at home on Census night. If you are living in a group house, or wish to keep your information private from others in your household, go to www.census.abs.gov.au.*[38] *A range of different self-service options are available to help you complete your Census form.* The ABS has also advised that they plan to add specific wording to the online form reminding the head of the household that individual forms should be offered to household members if they prefer. Similar wording will be added to the paper form.
C. Does the entity provide notice of the fact that the collection is required or authorised? (if relevant)	**Compliant**	[Refer to E below]
D. Does the entity provide notice of the purpose of collection?	**Compliant**	The draft Census privacy collection notice states: *For the Census we collect and hold the following kinds of personal information about you:* ● *name* ● *address* ● *basic demographics (e.g. age, sex, marital status, relationship with other household members)* ● *personal characteristics (e.g. date of birth, country of birth, languages spoken, education qualification, employment information and income)* ● *sensitive personal information including racial or ethnic origin, religious beliefs (optional) and long-term health conditions.* *We collect personal information such as phone numbers and emails to provide services to help us run the Census. We do not keep that information past the Census collection period, which usually ends by October 2021.*
E. Does the entity provide notice of the main consequences (if any) for the individual if all or some of the personal information is not collected?	**Action required**	APP 5 requires consumers to be informed about the consequences of not providing information. This is a complex issue for the Census and requires careful consideration. Completing the Census is mandatory, but there are only potential consequences once an individual has received a formal Notice of Direction. The ABS has to tread a fine line between encouraging participation and providing realistic information about the consequences for not responding. This issue (notice of consequences) is closely tied to broader issues regarding the mandatory nature of the Census (discussed below, refer to Section 22. Additional Governance Requirements). **Recommendation 3: Clarify privacy notice information on the potential consequences for not providing information** The ABS should develop a clear and consistent set of wording to inform consumers about the consequences of not completing the Census.

[38] Note: this link will be available from mid-October 2020.

		Note: At the time of completing this PIA the ABS has drafted a Census privacy notice which states: *The Census is conducted under the authority of the Census and Statistics Act 1905. If you refuse to complete your Census form, the Australian Statistician has the power to direct you to do so. We seek your willing participation first, but if you continue to refuse, even after receiving a Notice of Direction from the Statistician, you may have to go to Court. You could be fined and receive a criminal conviction.* The ABS has also advised that they are collating a comprehensive table of all the wording used for refusals (across multiple documents). This will assist in creating consistent wording regarding the consequences of not completing the Census.
F. Does the entity provide notice of any other APP entity, body or person, or the types of any other APP entities, bodies or persons, to which the APP entity usually discloses personal information of the kind collected?	**Compliant**	The draft Census privacy notice includes information on the four 'data pathways' for Census data, including the types of entities who might receive de-identified Census data (e.g. researchers) or in very limited circumstances, identified data (e.g. the storing of the Time Capsule by the National Archives of Australia).
G. Does the entity provide notice that the privacy policy contains information about how the individual may access their personal information and seek the correction of such information?	**Compliant** **Further measures possible**	The draft Census privacy notice states: ***How to access and correct your personal information*** *Contact the ABS using the details provided below if you need to access or correct personal information collected about you in relation to supporting Census operations. It is not possible to access or change information on a Census form that has been submitted.* **Note:** This is an area where there is a need for greater clarity and improvement – Refer to Recommendation 7: Clarify access rules for different categories of data in APP 12 below.
H. Does the entity provide notice that the privacy policy contains information about how the individual may complain?	**Compliant**	The draft Census privacy notice contains a detailed section on privacy complaints.
I. Does the entity provide notice of whether the entity is likely to disclose the personal information to overseas recipients (and if so, where)?	**Compliant**	n/a

11.3. APP 5. Finding

Overall, this PIA has found that the compliance status for APP 5 is: Action required.

12. APP 6. Use or Disclosure of Personal Information

12.1. APP 6. The Law

APP 6 — use or disclosure of personal information

Use or disclosure

6.1 If an APP entity holds personal information about an individual that was collected for a particular purpose (the primary purpose), the entity must not use or disclose the information for another purpose (the secondary purpose) unless:

> *(a) the individual has consented to the use or disclosure of the information; or*
>
> *(b) subclause 6.2 or 6.3 applies in relation to the use or disclosure of the information.*

Note: APP 8 sets out requirements for the disclosure of personal information to a person who is not in Australia or an external Territory.

6.2 This subclause applies in relation to the use or disclosure of personal information about an individual if:

> *(a) the individual would reasonably expect the APP entity to use or disclose the information for the secondary purpose and the secondary purpose is:*
>
> > *(i) if the information is sensitive information — directly related to the primary purpose; or*
> >
> > *(ii) if the information is not sensitive information — related to the primary purpose; or*
>
> *(b) the use or disclosure of the information is required or authorised by or under an Australian law or a court/tribunal order; or*
>
> *(c) a permitted general situation exists in relation to the use or disclosure of the information by the APP entity; or*
>
> *(d) the APP entity is an organisation and a permitted health situation exists in relation to the use or disclosure of the information by the entity; or*
>
> *(e) the APP entity reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body.*
>
> *Note: For **permitted general situation**, see section 16A. For **permitted health situation**, see section 16B.*

...

Written note of use or disclosure

6.5 If an APP entity uses or discloses personal information in accordance with paragraph 6.2(e), the entity must make a written note of the use or disclosure.

12.2. APP 6. OAIC Guidelines

The *PIA Guidelines* issued by the Office of the Australian Information Commissioner (OAIC) contain a set of hints and risks under the category of purpose, use and disclosure.

The Privacy hints they have identified include:

- No surprises! Use personal information in ways that are expected by the individual
- No surprises! Tell the individual about disclosures.

The Privacy Risks they have identified include:

- Using personal information for unexpected secondary purposes
- Unnecessary or unexpected data linkage
- Unexpected disclosures can lead to privacy complaints.

More information: <www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-6-app-6-use-or-disclosure-of-personal-information>.

The OAIC has provided additional guidance about data analytics:

- *De-identification and the Privacy Act*, Office of the Australian Information Commissioner (OAIC), March 2018 <www.oaic.gov.au/privacy/guidance-and-advice/de-identification-and-the-privacy-act>
- *Guide to Data Analytics and the Australian Privacy Principles*, Office of the Australian Information Commissioner (OAIC), March 2018 <www.oaic.gov.au/privacy/guidance-and-advice/guide-to-data-analytics-and-the-australian-privacy-principles>
- *De-identification Decision-Making Framework*, Office of the Australian Information Commissioner (OAIC) and Data61 (CSIRO), September 2017 <www.oaic.gov.au/privacy/guidance-and-advice/de-identification-decision-making-framework>

12.3. APP 6. 2021 Census – Overview

The following table summarises the key compliance tasks relevant to APP 6:

APP 6. Use or Disclosure	Action / Status	Galexia Commentary
A. Has the entity clearly defined the primary purpose of collection and identified any secondary purposes?	**Compliant**	The ABS has clearly identified four primary purposes (or 'data pathways') for Census data. These primary purposes are all authorised in ABS and Census legislation and are clearly notified to consumers. Some limited secondary purposes have been identified and these are also clearly authorised in legislation and notified to consumers. These include: ● Managing and planning the Census; ● Evaluating the quality of Census data; and ● Managing consumer inquiries and complaints.
B. Will the entity only disclose personal information for a secondary purpose with consent (or a relevant exception)?	**Compliant**	APP 6 generally allows the use and disclosure of information where a legal authority exists for that use or disclosure. This rule applies to the use and disclosure of Census data (e.g. for statistical publications or data integration purposes), but is 'trumped' by the more restrictive provisions of the Census legislation. Under the Census legislation, the ABS cannot release information that is likely to identify an individual. Some external stakeholders have raised concerns with the methods that the ABS uses to de-identify information before making it available to researchers. However, this PIA recommends that the ABS continues to use a layered approach to managing re-identification risk. This PIA makes some suggested enhancements to this approach in Structural Recommendation 3: Principles based approach to managing re-identification risk. In addition, some Census data is disclosed to the Time Capsule maintained by the National Archives. This data will be released to the public 99 years after its initial collection. This use and disclosure requires the specific consent of data subjects.

C. Is any biometric information only disclosed for a secondary purpose in accordance with Clause 6.3 and the relevant OAIC Guidelines?	**Compliant**	n/a
D. Is a written note made of any disclosures that are made relying on the law enforcement exception?	**Compliant**	Census data (i.e. the statistical data that is submitted on the Census form) that might identify an individual is never disclosed to law enforcement agencies. Some data regarding individuals that is collected during the administration of the Census may be disclosed to law enforcement – e.g. where a member of the public threatens a Census field officer. In those rare cases no statistical data is disclosed. A formal record of the proceedings and communications is maintained by the ABS.

12.4. APP 6. Finding

Overall, this PIA has found that the compliance status for APP 6 is: Compliant.

13. APP 7. Direct Marketing

13.1. APP 7. The Law

APP 7 provides that an organisation must not use or disclose personal information it holds for the purpose of direct marketing unless an exception applies.

More information: <www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-7-app-7-direct-marketing>.

13.2. APP 7. 2021 Census – Overview

The following table summarises the key compliance tasks relevant to APP 7:

APP 7. Direct Marketing	Action / Status	Galexia Commentary
A. An organisation must not use or disclose personal information it holds for the purpose of direct marketing unless an exception applies	**Compliant**	The ABS is prohibited from releasing information that is likely to identify an individual.[39] As a result, no Census information is disclosed for the purpose of direct marketing.

13.3. APP 7. Finding

Overall, this PIA has found that the compliance status for APP 7 is: Compliant.

[39] Sections 12 and 13 of *Census and Statistics Act 1905 (Cth)* <www.legislation.gov.au/Details/C2016C01005>.

14. APP 8. Cross-border Disclosure of Personal Information

14.1. APP 8. The Law

APP 8 states that before an organisation discloses personal information to an overseas recipient, they must take reasonable steps to ensure that the overseas recipient does not breach the APPs in relation to the information. The organisation that discloses personal information to an overseas recipient is accountable for any acts or practices of the overseas recipient. Several exceptions apply.

APP 8 — Cross-border disclosure of personal information

*8.1 Before an APP entity discloses personal information about an individual to a person (the **overseas recipient**):*

(a) who is not in Australia or an external Territory; and

(b) who is not the entity or the individual;

the entity must take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the Australian Privacy Principles (other than Australian Privacy Principle 1) in relation to the information.

8.2 Subclause 8.1 does not apply to the disclosure of personal information about an individual by an APP entity to the overseas recipient if:

(a) the entity reasonably believes that:

(i) the recipient of the information is subject to a law, or binding scheme, that has the effect of protecting the information in a way that, overall, is at least substantially similar to the way in which the Australian Privacy Principles protect the information; and

(ii) there are mechanisms that the individual can access to take action to enforce that protection of the law or binding scheme; or

(b) both of the following apply:

(i) the entity expressly informs the individual that if he or she consents to the disclosure of the information, subclause 8.1 will not apply to the disclosure;

(ii) after being so informed, the individual consents to the disclosure; or

(c)-(f) [Note: several additional exceptions apply]

More information: <www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-8-app-8-cross-border-disclosure-of-personal-information>.

14.2. APP 8. 2021 Census – Overview

The following table summarises the key compliance tasks relevant to APP 8:

APP 8. Cross-border Disclosure	Action / Status	Galexia Commentary
A. Has the entity identified all relevant cross-border disclosure of personal information?	**Compliant**	The ABS will not process, store or transfer any information from the 2021 Census outside Australia. The ABS has included a prohibition on cross-border data transfers in its agreements with third party service providers.

B. Has the entity taken such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the APPs? (unless a relevant exception applies)	**Compliant**	n/a

14.3. APP 8. Finding

Overall, this PIA has found that the compliance status for APP 8 is: Compliant.

15. APP 9. Adoption, Use or Disclosure of Government Related Identifiers

15.1. APP 9. The Law

APP 9 states that an organisation must not adopt a government related identifier of an individual as its *own* identifier. In addition, an organisation must not use or disclose a government related identifier of an individual unless the use or disclosure is reasonably necessary for the organisation to verify the identity of the individual. Some other exceptions apply.

More information: <www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-9-app-9-adoption-use-or-disclosure-of-government-related-identifiers>.

15.2. APP 9. Census 2021 – Overview

The following table summarises the key compliance tasks relevant to APP 9:

APP 9. Government Related Identifiers	Action / Status	Galexia Commentary
A. An organisation must not adopt a government related identifier as their own identifier.	**Compliant**	APP 9 does not generally apply to agencies apart from some prescribed commercial activities undertaken by agencies. However, this APP is designed to prevent the development of de-facto national identifiers, so it is good practice for all entities to follow it. APP 9 has very limited application to the 2021 Census. Government related identifiers do not play a direct role in the collection, use and disclosure of information in the Census. The ABS does use a unique Census Number on forms and letters that identifies the relevant household. This plays an important role in reconciling multiple forms that might relate to the same household or individual, but it is not used in general processing of Census data. Similarly the ABS issues a unique temporary password for households and individuals who wish to complete the Census using the online service. This code plays an important role in managing data entry and reconciliation, but is not subsequently used in processing Census data.
B. Government related identifiers should not be disclosed except in specific situations (e.g. where the disclosure is reasonably necessary to verify identity)	**Compliant**	APP 9 does not generally apply to agencies apart from some prescribed commercial activities undertaken by agencies. The ABS may incidentally use a government related identifier as part of its identity linking process in the Multi-Agency Data Integration Project (MADIP), however these are never disclosed by the ABS to any external parties.

15.3. APP 9. Finding

Overall, this PIA has found that the compliance status for APP 9 is: Compliant.

16. APP 10. Quality of Personal Information

16.1. APP 10. The Law

APP 10 — quality of personal information

10.1 An APP entity must take such steps (if any) as are reasonable in the circumstances to ensure that the personal information that the entity collects is accurate, up-to-date and complete.

10.2 An APP entity must take such steps (if any) as are reasonable in the circumstances to ensure that the personal information that the entity uses or discloses is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant.

16.2. APP 10. OAIC Guidelines

The *PIA Guidelines* issued by the Office of the Australian Information Commissioner (OAIC) contain a set of hints and risks under the category of data quality.

The Privacy Risks they have identified include:

- Retaining personal information unnecessarily
- Making decisions based on poor quality data.

More information: <www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-10-app-10-quality-of-personal-information>.

16.3. APP 10. 2021 Census – Overview

The following table summarises the key compliance tasks relevant to APP 10:

APP 10. Data Quality	Action / Status	Galexia Commentary
A. Has the entity taken such steps (if any) as are reasonable in the circumstances to ensure that the personal information **collected** is accurate, up-to-date and complete?	**Compliant**	Data quality is an important issue for the Census. A Post Enumeration Survey is conducted after each Census and a report on Data Quality is published. The 2016 Census Data Quality Report[40] found that data quality was acceptable for the objectives of the ABS and its clients. Lessons learned from that report are being implemented by the ABS for the 2021 Census. One suggested measure to improve data quality is the potential use of some administrative data for the 2021 Census. This issue is the subject of a separate stand-alone Privacy Impact Assessment and is not the subject of detailed discussion in this PIA.

[40] Census Independent Assurance Panel (CIAP) to the Australian Statistician, *Report on the Quality of 2016 Census Data* (July 2017) <www.abs.gov.au/websitedbs/d3310114.nsf/Home/Independent+Assurance+Panel>.

		Briefly, the ABS has a Census Futures project that is examining the potential use of administrative data in three scenarios: 1) **Maximising the Census response** Using admin data to help the ABS identify localities that require additional or specific forms of support to participate in the Census (for example, the ABS may endeavour to provide more hard copy forms to an area with a high proportion of older Australians). 2) **Improving the Census count** Using admin data to better determine whether a house that did not return a Census form was occupied on Census night and using the data to choose more compatible 'donor houses'. 3) **Repairing the Census** In the event of a natural disaster or an across the board low response to the Census, using admin data to repair Census data. The results of the separate PIA on the use of admin data can be viewed on the ABS public PIA Register.[41]
B. Has the entity taken such steps (if any) as are reasonable in the circumstances to ensure that the personal information **that the entity uses or discloses** is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant?	**Compliant**	Key ABS statistical publications and services (e.g. TableBuilder) are accompanied by a guide to methodology and data quality. This helps users and researchers understand the level of accuracy that can be expected from the published data. For Census data there is a trade-off between data quality and protecting privacy. In order to avoid disclosing information that might identify an individual, many ABS publications and services have deliberately reduced the accuracy of the data. This is an acceptable practice under the *Privacy Act,* as the data is still accurate 'having regard for its use'.

16.4. APP 10. Finding

Overall, this PIA has found that the compliance status for APP 10 is: Compliant.

[41] <www.abs.gov.au/websitedbs/D3310114.nsf/home/ABS+Privacy+Impact+Assessments>

17. APP 11. Security of Personal Information

17.1. APP 11. The Law

APP 11 requires organisations to take such steps as are reasonable in the circumstances to protect personal information from misuse, interference and loss; and from unauthorised access, modification or disclosure.

Also, if the organisation no longer needs the information for any purpose for which the information may be used or disclosed, they must take such steps as are reasonable in the circumstances to destroy the information or to ensure that the information is de-identified.

APP 11 — Security of personal information

11.1 If an APP entity holds personal information, the entity must take such steps as are reasonable in the circumstances to protect the information:

> *(a) from misuse, interference and loss; and*
>
> *(b) from unauthorised access, modification or disclosure.*

11.2 If:

> *(a) an APP entity holds personal information about an individual; and*
>
> *(b) the entity no longer needs the information for any purpose for which the information may be used or disclosed by the entity under this Schedule; and*
>
> *(c) the information is not contained in a Commonwealth record; and*
>
> *(d) the entity is not required by or under an Australian law, or a court/tribunal order, to retain the information;*

the entity must take such steps as are reasonable in the circumstances to destroy the information or to ensure that the information is de–identified.

17.2. APP 11. OAIC Guidance

APP 11 has a very wide scope for interpretation, as it includes multiple tests for what is 'reasonable in the circumstances'. Some additional guidance is available from the Office of the Australian Information Commissioner (OAIC) in the form of guidelines:

- *Guide to securing personal information*, OAIC, 2015 <www.oaic.gov.au/privacy/guidance-and-advice/guide-to-securing-personal-information>

More information: <www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-11-app-11-security-of-personal-information>.

17.3. APP 11. 2021 Census – Overview

This PIA is not a full security assessment of the 2021 Census. As discussed below, the ABS has commissioned a range of comprehensive security reviews.

The ABS applies a layered approach to security for Census data, with an emphasis on:

1) Protecting the data while it is in its raw identified form (e.g. on Census forms, or during online submission);
2) Applying robust separation measures to the data while it is being processed, so that name and address data is kept separate from other Census content; and
3) Ensuring that data outputs such as statistical publications or data made available to researchers are unlikely to identify an individual.

The following table provides a very high level summary of ABS compliance with APP 11 regarding the 2021 Census:

APP 11. Security	Action / Status	Galexia Commentary
A. Has the entity taken such steps as are reasonable in the circumstances to protect the information from misuse, interference, loss, unauthorised access, modification or disclosure?	**In progress**	The data being collected, used and disclosed in the 2021 Census includes highly sensitive data. The scale of the data involved is also significant. It will be important for security settings to match the potential harm of any breaches. The ABS finalised the *2021 Census – Security Strategy (IT Security)*[42] in January 2020. This provides a high level approach to identifying and managing security risks. The ABS has not undertaken a comprehensive independent security risk assessment for the 2021 Census as of April 2020, although an 'end to end' security risk assessment has been commissioned. **Recommendation 4: Conduct independent security risk assessments for key 2021 Census components** The ABS should commission independent security risk assessments for key components of the 2021 Census: ● An 'end to end' assessment (this has been commissioned); ● A specific assessment of the cloud platform (this may be covered by existing security certifications); and ● The Time Capsule (this has yet to be commissioned). During the development of this PIA, Galexia has recommended that further specific security risk assessments be conducted on two key areas: **The Cloud platform**[43] – This is an important step because: ● The majority of households are expected to complete the Census online; ● The online Census service was the subject of an external attack in 2016; and ● A new Cloud provider has been selected to work with the ABS on the 2021 Census. **The Time Capsule** – This is an important step because: ● It will contain roughly 50% of 2021 Census data; ● It contains multiple years of data; ● It contains names and addresses; ● It requires secure transfer; and ● It is maintained by a third party.
B. Does the level of security in the application match the potential harm caused by breaches of privacy?	**In progress**	This issue will be assessed as part of the independent security review discussed above.
C. Will detailed access trails be retained and scrutinised for security breaches?	**In progress**	This issue will be assessed as part of the independent security review discussed above.

[42] ABS, *2021 Census – Security Strategy (IT Security)*, v1.0 January 2020 [Internal document]

[43] ABS, *Media Release: ABS appoints PwC Australia and The Adecco Group Australia to deliver key 2021 Census services* (3 May 2019) <www.abs.gov.au/ausstats/abs%40.nsf/mediareleasesbyCatalogue/4D95297065D18DA2CA2583EE0080A857>

D. Will a data retention policy / destruction schedule be developed which requires retention of personal information only for the period required for use? **Names**	**Action required**	APP 11 requires the ABS to destroy or de-identify data as soon as there is no business purpose for retaining it. This is also best practice in reducing the security risk profile of large datasets. In 2016 the ABS decided to retain names and addresses for four years or for as long as required (whichever was shorter). In practice, names were deleted after three years and addresses will be deleted closer to the four year deadline. As the Census is conducted every five years there is a risk that this approach amounts to a de-facto permanent retention of identifying data, forming a significant national dataset that is held almost indefinitely. This is not the objective of the Census. During discussions with ABS teams during the development of this PIA it has become clear that the time required for keeping names could be much shorter. Names are useful in reconciling duplicates and gaps in coverage and play an important role in data quality. (Refer to the 2021 Census Privacy Statement[44] for examples of how the ABS uses name and address information). Activities that require names are generally completed shortly after data collected in the Census is processed for publication and used to help plan the subsequent (eg 2026) Census. Names do play a role in data integration, but no compelling reason was presented for retention of names for such a lengthy period. ABS Data Integration uses the Census as a 'snapshot' and not as a longitudinal product. Overall, data integration should not be allowed to 'drive' the collection of additional data or the retention of data that would otherwise be destroyed. The long-term retention of names presents an unacceptable level of privacy and security risk for the Census, and may undermine other privacy measures. This PIA recommends a significant overhaul of the approach to name retention. **Recommendation 5: Shorten data retention periods for names** The ABS should review and significantly reduce the data retention periods for names. If the reduction needs to be staggered to meet business needs, this should be reduced over the next two Censuses. As a minimum the data retention period for names should be re-set as 18 months for the 2021 Census.

[44] The Privacy Statement will be available at <www.census.abs.gov.au/privacy> from mid-October 2020. During the PIA process the Census Privacy Team conducted an investigation into the length of time names and addresses are proposed to be retained by the ABS from the 2021 Census. Teams undertaking core Census activities, data integration and other activities that rely on names and addresses from the Census identified how the names and/or addresses are used, and the length of time taken to complete these activities.

ABS considered:

- Census activities that include coding and processing to produce Census data for release to the public and internal activities to prepare for the next Census including updating of indexes and system testing.
- Other (non-Census) teams which use either names and/or addresses for a range of activities including data integration and input to Closing the Gap reporting.

E. Will a data retention policy / destruction schedule be developed which requires retention of personal information only for the period required for use? **Addresses**	**Action required**	Retention of address data may provide some additional assistance in Census planning and data quality measures. But again, no justification was presented for the long-term retention of all addresses. The decision to retain addresses was made in the context of the ABS developing an Address Register and generally changing its approach to addresses. The lengthy retention of address information for future Censuses is difficult to justify. In addition, the Census collects five different addresses for each individual: 1) Address on Census night; 2) Current residential address; 3) Residential address one year ago; 4) Residential address five years ago; and 5) Employer address. During the PIA process, the ABS has consulted with internal teams and developed a list of timing requirements for addresses. Addresses are required for slightly longer than names – around two years. Some further benefits would be gained from holding addresses for an even longer period for planning for the 2026 Census, but no longer than three years. The long-term retention of addresses presents an unacceptable level of privacy and security risk for the Census, and may undermine other privacy measures. This PIA recommends a significant overhaul of the approach to address retention. **Recommendation 6: Shorten data retention periods for addresses** The ABS should review and, if possible, reduce the data retention periods for addresses. If the reduction needs to be staggered to meet business needs, this should be reduced over the next two Censuses. As a minimum the data retention period for addresses should be reduced for the 2021 Census to a period of 24-36 months. **Note:** The ABS has created a table illustrating the different name and address retention requirements relating to Census and non-Census use. (Refer to the 2021 Census Privacy Statement[45] for examples of how the ABS uses name and address information).
F. Is personal information de-identified as soon as possible?	**Action required**	Refer to Recommendation 5 and Recommendation 6 above.

17.4. APP 11. Finding

Overall, this PIA has found that the compliance status for APP 11 is: Action Required.

[45] Ibid.

18. APP 12. Access to Personal Information

18.1. APP 12. The Law

APP 12 — access to personal information

Access

12.1 If an APP entity holds personal information about an individual, the entity must, on request by the individual, give the individual access to the information.

Exceptions to access...

More information: <www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-12-app-12-access-to-personal-information>.

18.2. APP 12. 2021 Census – Overview

The following table summarises the key compliance tasks relevant to APP 12:

APP 12. Access	Action / Status	Galexia Commentary
A. Can the individual ascertain whether the entity has records that contain personal information, the nature of that information and the steps that the individual should take to access their record?	**Action required**	The ABS has access policies and procedures in place for its own data that are compliant with APP 12. The ABS also has a special *Privacy Act 1988* and *Freedom of Information Act 1982* exemption available for access requests in relation to data that it has collected for statistical purposes. However, in relation to the 2021 Census there is a lack of clarity over what data may be the subject of access requests (noting that exemptions are clearly available for access to some of these datasets, but these exemptions are not mentioned in the current privacy policy.[46] They are briefly mentioned in the draft Census privacy notice.[47]) **Recommendation 7: Clarify access rules for different categories of data** The ABS should clarify the access rules that apply to each category of data, and set these out clearly in the 2021 Census Privacy Policy, including: • Core Census data (i.e. statistical data); • ACLD; • Integrated Census data (e.g. MADIP); • Time Capsule; and • Other non-statistical data (e.g. Contact Centre records).

[46] ABS, *Privacy Policy* (6 January 2020) <www.abs.gov.au/websitedbs/D3310114.nsf/Home/Privacy+Policy>

[47] ABS, *Collection of your personal information in the 2021 Census of Population and Housing* (24 April 2020) [internal working document]

A. (continued)	**Action required**	In addition, rules around access to Time Capsule data may need to be clarified and strengthened following international experiences. In the UK, for example, access to Time Capsule data has been the subject of significant legal disputes, and some data has been released early following a successful Freedom of Information request.[48] It is important to learn lessons from this international experience and review the Time Capsule arrangements to ensure that there is **no possibility** of early release of Census data. **Recommendation 8: Clarify and strengthen access restrictions to data held in the Time Capsule** The ABS should clarify and strengthen access rules that apply to data held in the Time Capsule, noting examples of international pressure for early access to similar data.
B. If an agency holds personal information about an individual, does the agency, on request by the individual, give the individual access to the information? (unless relevant exceptions apply)	**Compliant**	[Refer to the discussion of potential exemptions above in A.]
C. Will information be provided within 30 days?	**Compliant**	Where an access request is granted, the ABS will comply with the 30 day rule.
D. Will accessing personal information be provided at no cost?	**Compliant**	Where an access request is granted, the ABS will comply with the relevant charging rules.

18.3. APP 12. Finding

Overall, this PIA has found that the compliance status for APP 12 is: Action Required.

[48] United Kingdom Information Commissioner's Office (ICO) <ico.org.uk>, N*ational Archives (Decision Notice) [2006] UKICO FS50101391* (11 December 2006) <www.bailii.org/uk/cases/UKICO/2006/FS50101391.html>

19. APP 13. Correction of Personal Information

19.1. APP 13. The Law

APP 13 — correction of personal information

Correction

13.1 If:

> *(a) an APP entity holds personal information about an individual; and*
>
> *(b) either:*
>
> > *(i) the entity is satisfied that, having regard to a purpose for which the information is held, the information is inaccurate, out of date, incomplete, irrelevant or misleading; or*
> >
> > *(ii) the individual requests the entity to correct the information;*
>
> *the entity must take such steps (if any) as are reasonable in the circumstances to correct that information to ensure that, having regard to the purpose for which it is held, the information is accurate, up to date, complete, relevant and not misleading.*

Notification of correction to third parties

13.2 If:

> *(a) the APP entity corrects personal information about an individual that the entity previously disclosed to another APP entity; and*
>
> *(b) the individual requests the entity to notify the other APP entity of the correction;*

the entity must take such steps (if any) as are reasonable in the circumstances to give that notification unless it is impracticable or unlawful to do so.

...

Dealing with requests

13.5 If a request is made under subclause 13.1 or 13.4, the APP entity:

> *(a) must respond to the request:*
>
> > *(i) if the entity is an agency — within 30 days after the request is made; or*
> >
> > *(ii) if the entity is an organisation — within a reasonable period after the request is made; and*
>
> *(b) must not charge the individual for the making of the request, for correcting the personal information or for associating the statement with the personal information (as the case may be).*

19.2. APP 13. OAIC Guidelines

The *PIA Guidelines* issued by the Office of the Australian Information Commissioner (OAIC) contain a set of hints and risks under the category of correction of personal information.

- Getting access to personal information should be clear and straightforward.
- Inaccurate information can cause problems for everyone!

More information: <www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-13-app-13-correction-of-personal-information>.

19.3. APP 13. 2021 Census – Overview

The following table summarises the key compliance tasks relevant to APP 13:

APP 13. Correction	Action / Status	Galexia Commentary
A. UPON REQUEST Does the entity take such steps (if any) as are reasonable in the circumstances to correct that information?	**Compliant**	The ABS is exempt from the correction requirements in relation to statistical data collected in the Census. However, it is covered by the correction requirements for other data (e.g. data provided via the Contact Centre). The current draft of the Census privacy notice[49] states: ***How to access and correct your personal information*** *Contact the ABS using the details provided below if you need to access or correct personal information collected about you in relation to supporting Census operations. It is not possible to access or change information on a Census form that has been submitted.*
B. UPON LEARNING OF INACCURACIES Does the entity take such steps (if any) as are reasonable in the circumstances to correct that information? (where the inaccuracy relates to a purpose for which the information is held)	**Compliant**	The ABS is exempt from the correction requirements in relation to statistical data collected in the Census. However, it is covered by the correction requirements for other data (e.g. data provided via the Contact Centre).
C. UPON REQUEST ONLY Will corrections and annotations be disseminated to third parties to whom personal information has previously been disclosed?	**Compliant**	ABS complies with this requirement for non-statistical data.
D. Will requests for corrections be addressed within 30 days?	**Compliant**	ABS complies with this requirement for non-statistical data.

19.4. APP 13. Finding

Overall, this PIA has found that the compliance status for APP 13 is: Compliant.

[49] ABS, *Collection of your personal information in the 2021 Census of Population and Housing* (24 April 2020) [internal working document]

20. ABS Legislation

This PIA also assesses the 2021 Census implementation against ABS legislation.

The following table summarises high level findings on compliance with ABS legislation:

Action / Status	Galexia Commentary	Galexia Recommendation
***Census and Statistics Act 1905* (Cth)**		
Compliant	General Census use and disclosure must comply with the objectives of the *Census and Statistics Act 1905 (Cth)*.[50] Section 8 of this Act specifically authorises the Census. Section 8a authorises the Time Capsule. The Act contains a prohibition on releasing any data in a manner that is likely to enable the identification of a particular person. The Act also contains significant penalties and sanctions for releasing data. The ABS has taken steps to ensure that all persons and partners engaged in the Census are covered by these provisions (for example, field workers become temporary employees of the ABS). Some external stakeholders have raised concerns with the methods that ABS uses to de-identify information before making it available to researchers.	However, this PIA recommends that the ABS continues to use a layered approach to managing re-identification risk. This PIA makes some suggested enhancements to this approach in Structural Recommendation 3: Principles based approach to managing re-identification risk.
***Australian Bureau of Statistics Act 1975* (Cth)**		
Compliant	The *Australian Bureau of Statistics Act 1975 (Cth)*[51] allows the ABS to both collect data and integrate data with other data holdings (Section 6). This Act allows Census data to be included in integrated data assets such as MADIP. When Census data is used in MADIP, the Accredited Integrating Authority (the ABS) is subject to the prohibition on releasing any data in a manner that is likely to enable the identification of a particular person. Some external stakeholders have raised concerns with the methods that ABS uses to encode names so that Census data can be linked to other datasets. Generally, there was a poor level of understanding regarding name encoding, and some stakeholders erroneously presumed that the ABS used a simple, reversible linking process – such as a Statistical Linkage Key (SLK). Other stakeholders understood the more complex process actually used by the ABS (Lossy encoding), but still had some concerns about the integrity and risks of this approach.	This PIA recommends that the ABS adopts a new principles based approach to name encoding in Structural Recommendation 2: Principles based approach to name encoding for data linkage.

Overall, this PIA has found that the compliance status for ABS Legislation is: Compliant.

[50] <www.legislation.gov.au/Details/C2016C01005>

[51] <www.legislation.gov.au/Details/C2019C00184>

21. Australian Government Agencies Privacy Code

Australian Government Agencies are bound by the privacy governance requirements set out in the *Privacy (Australian Government Agencies — Governance) APP Code 2017.*[52] The Code was registered on 27 October 2017 and commenced on 1 July 2018.

The Code requirements apply to the ABS. It is likely that over time they will be applied to all ABS contractors. For the ABS they will apply as a whole, rather than to the 2021 Census specifically. In this PIA, Galexia has applied the Code requirements as a guide to privacy governance best practice.

The following table summarises the key privacy governance obligations:

APS Privacy Code Requirements	APP Code Section	Action / Status	APS Privacy Code Detailed Requirements	Galexia Commentary and Recommendations
A. Privacy Management Plan	**9**	**Compliant**	An agency must have a Privacy Management Plan that: • identifies specific, measurable privacy goals and targets; and • sets out how an agency will meet its compliance obligations under APP 1.2.	A comprehensive Privacy Management Plan was published in 2018 and is being updated for 2019. The Plan was examined as part of the PIA process and clearly complies with the Code requirements. However, the Plan covers the ABS as a whole, and is not specific to the Census. This PIA recommends that the ABS adopts a new 7-8 year Census privacy Strategy, covering more than one Census period. Refer to Structural Recommendation 1: Census Privacy Strategy, which includes a proposed table of privacy goals and targets that are specific to the Census.
B. Privacy officer	**10**	**Compliant**	An agency must appoint a Privacy Officer and ensure that particular Privacy Officer functions are undertaken.	A Chief Privacy Officer has been designated.
C. Privacy champion	**11**	**Compliant**	An agency must appoint a senior official as a Privacy Champion to provide cultural leadership and promote the value of personal information.	An ABS Privacy Champion has been in place for two years and plays an active role in the 2021 Census planning.

[52] The *Australian Government Agencies Privacy Code*, <www.oaic.gov.au/privacy-law/australian-government-agencies-privacy-code>.

D. PIAs	**12**	**In Progress**	An agency must undertake a written Privacy Impact Assessment (PIA) for all 'high privacy risk' projects or initiatives that involve new or changed ways of handling personal information.	ABS undertakes regular PIAs.[53] In relation to the Census the key PIAs are: • 2016 Census (internal); • MADIP PIA 2017 (independent); • MADIP PIA Update 2019 (mixed internal and external); • Potential use of administrative data in the 2021 Census (independent); and • 2021 Census (independent) (this document). However, it is important not to assume that this Code requirement does not apply to prior initiatives. If a prior initiative is to be renewed, and has a significant privacy risk profile, then the ABS should consider conducting a new PIA. In relation to the Census, the ABS could consider conducting additional independent PIAs for: • The ACLD; and • The Time Capsule.[54] These activities are 'renewed' for each Census, but Census questions and other policy settings (e.g. data retention, security and third party involvement) may have changed. **Recommendation 9: Conduct additional independent PIAs for activities that are 'renewed' for each Census** The ABS should consider conducting additional independent PIAs for the ACLD and the Time Capsule.
E. PIA register	**15**	**Compliant**	An agency must keep a register of all PIAs conducted and publish this register, or a version of the register, on the agency website.	The ABS maintains a public PIA Register.[55]
F. Privacy training	**16**	**Compliant**	An agency must enhance internal privacy capability, including by providing appropriate privacy education or training in staff induction programs, and annually to all staff who have access to personal information.	ABS has comprehensive policies and procedures in place on privacy training, awareness raising and capacity building. Under the leadership of the Privacy Champion, the establishment of a privacy culture at the ABS is a priority.

[53] <www.abs.gov.au/websitedbs/D3310114.nsf/home/ABS+Privacy+Impact+Assessments>

[54] The MacGibbon review of the 2016 Census recommended that:

> *The ABS should ensure future significant changes to personal information handling practices are subject to an **independently-conducted** privacy impact assessment.*

Review of the events surrounding the 2016 eCensus: Improving institutional cyber security culture and practices across the Australian government – Alastair MacGibbon, Special Adviser to the Prime Minister on Cyber Security – Department of the Prime Minister and Cabinet – 13 October 2016
<parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id:%22publications/tabledpapers/a41f4f25-a08e-49a7-9b5f-d2c8af94f5c5%22>

[55] <www.abs.gov.au/websitedbs/D3310114.nsf/home/ABS+Privacy+Impact+Assessments>

G. Monitoring and review	**17**	**Compliant**	An agency must regularly review and update its privacy practices, procedures and systems, and an agency must monitor compliance with its privacy practices, procedures and systems regularly.	In addition to the general ABS Privacy Management Plan (which is monitored and reviewed every year), the Census has its own High Level Privacy Work Plan that is monitored and reviewed six-monthly.

Overall, this PIA has found that the compliance status for Australian Government Agencies Privacy Code is: In Progress.

22. Additional Governance Requirements

The Census is a complex project and is subject to more than just compliance with the APPs and the Australian Government Agencies Privacy Code – and a broader governance framework is required.

The following table summarises (briefly) the core requirements that should be included in the ABS governance arrangements for the 2021 Census.

Additional Governance requirement	Action / Status	Galexia Commentary	Galexia Recommendation
A. Explaining the legal basis for data linkage	**Compliant** **Further measures possible**	The governance arrangements for the use of Census data in data integration are largely set out in MADIP policies and procedures. A public register of the legal basis for each MADIP partner agency to share data with MADIP has been established. A public register of any Public Interest Certificates issued by MADIP partner agencies is also available. However, one area of potential weakness is that the ABS policy on restricting linking Census data from prior Census collections (e.g. longitudinal study) via MADIP is not easily located. This policy should be prominent on information pages about both MADIP and the Census.	**Recommendation 10: Clarify the prohibition on using multiple Census collections in MADIP** The ABS should clarify and highlight the prohibition on using multiple Census collections for longitudinal study via MADIP.
B. Managing agreements with third parties and contractors	**In progress**	The ABS will be working with numerous third parties / contractors / partners for the implementation of the 2021 Census. Managing multiple third parties in a complex project can lead to privacy and security risks. During the PIA process, Galexia advised the ABS that the 2021 Census would benefit from the establishment of an internal register of all third parties, containing information on: • Nature of the agreement; • Expiry date or review / renewal / option date; • Applicable law; • Method for incorporating APPs; • Method for incorporating the ABS restriction on disclosure; • Restrictions on on-sharing or secondary use; • Rules for additional sub-contracting; • Security framework, standards, certifications; • Security audit requirement; • Security incident response; • Data breach notification requirement; • Restrictions on data being transferred overseas; and • Data destruction (or return) at end of agreement. The ABS has commenced work on the Register and will be able to use it to drive consistently high standards across agreements. There is no room for complacency or letting agreements 'drift' without appropriate oversight and review. Known partners or subcontractors include: • PWC Australia; • Amazon Web Services (AWS); • Adecco; • Payroll provider (EPI-USE); • MyWork App;	**Recommendation 11: Establish and maintain a register of third party agreements** The ABS should establish a register of third party agreements and use this to drive / promote a consistently high level of privacy protections and privacy management. **Note:** Work has commenced on this register and the issue is marked as 'in progress'.

		• Australia Post; • Mailing house service; • Service Australia Contact Centre; • MADIP Partners; and • National Archives of Australia (storage of Time Capsule).	
C. Managing Function Creep **Legislative basis for use of data**	**Action Required**	Several options for managing function creep are available. **Clarify legislative basis for use of data** This may seem like a strange requirement when the Census is heavily prescribed in legislation, but this issue was raised by stakeholders in response to the 2016 decision to retain name and address, and was also raised in an earlier Census PIA (2005).[56] The core question is not to identify the legal basis for *collecting* the data in the Census, but to place appropriate limits around what the data can then be *used* for. The 2005 Census PIA recommended: > ***Recommendation 3****: The ABS should consider seeking an amendment to the CSA to insert a definition of 'statistical purposes' to put beyond doubt that statistical purposes cannot include administrative, client management or law enforcement purposes that relate to specific individuals. A similar definition could usefully be inserted into the Australian Bureau of Statistics Act 1975.* This 2005 Recommendation remains valid. Indeed, there are now numerous examples of Commonwealth legislative frameworks that include a specific set of permitted and prohibited purposes for data. These include: • The Data Availability and Transparency Act (DATA) Framework (proposed); • *Treasury Laws Amendment (Consumer Data Right) Act 2019;* • *My Health Records Act 2012*; and • *Health Legislation Amendment (Data-matching and Other Matters) Act 2019*. It is important for the ABS to modernise its core legislation and add a specific section outlining the permitted and prohibited uses for the data that it collects.	**Recommendation 12: Clarify ABS legislation to set out permitted and precluded purposes for use of Census data** The ABS should explore ways to clarify legal restrictions on the use of Census data. Options might include a guideline, declaration or a potential legislative amendment.

[56] Pacific Privacy Consulting, *Census Enhancement Proposal: Privacy Impact Assessment Report for Australian Bureau of Statistics* (June 2005) <available from www.abs.gov.au/websitedbs/d3310114.nsf/home/abs+privacy+impact+assessments>.

D. Managing Function Creep **Application of the DATA Framework**	**Action Required**	Confidence in the privacy protections built into the Census may potentially be impacted by relying on the proposed Data Availability & Transparency Act (DATA) Framework to share or release data. That framework 'trumps' secrecy provisions in existing legislation, unless an Agency has succeeded in excluding itself from the framework. ABS is yet to establish a formal position on its involvement in the proposed DATA Framework. During the PIA, stakeholders expressed significant concerns regarding the potential relationship between the proposed DATA Framework and the Census. There was a sense from some key stakeholders that a detailed discussion of specific Census privacy protections was potentially 'moot' if those protections could just be over-ridden by the proposed DATA Framework. At the time of preparing this PIA, the DATA Bill has not been released for public comment. However, it is likely that there will be a process available for some agencies (or perhaps for specific datasets) to be exempted from the proposed DATA Framework. The Census is obviously a key national data asset and there will be pressure for it to be included in the proposed DATA Framework. This PIA can not provide a firm recommendation on the best way for ABS to approach this issue, but it was the number one concern raised by stakeholders, particularly privacy regulators. The ABS will need to engage in broad consultation before deciding to join the proposed DATA Framework. A decision to join the Framework would effectively replace the specific privacy protections set out in this PIA, with a separate approach based around: ● A purpose test; ● A list of prohibited purposes; ● An accreditation regime; ● Application of the Data Sharing Principles (in effect, a customised version of the Five Safes); ● Governance and oversight by the National Data Commissioner. This approach would be so different that the recommendations in this PIA would not be applicable. Although the DATA Framework may not be implemented for some time, it is likely to apply to some data collected prior to the passage of the legislation, and this could include data from the 2021 Census and previous Censuses. As well as over-riding the generic secrecy provisions that apply to ABS data, the DATA Framework could potentially over-ride some specific Census protections, such as the ABS policy that restricts the use of multiple Census data for longitudinal data linkage projects.	**Recommendation 13: Clarify the relationship between Census data and the proposed Data Availability and Transparency Act (DATA) Framework** The ABS should consider whether or not to exclude Census data from the proposed DATA Framework, and the potential impact of the DATA Framework on both the generic secrecy provisions that apply to ABS data and the specific privacy protections that apply to Census data.

E. Managing Function Creep **Application of the DATA Framework to the Time Capsule**	**Action Required**	This PIA is not the place to review all of the potential impacts of the proposed DATA Framework – especially as the Bill is not yet available. However, one specific impact that should be the subject of further examination is the potential for the proposed DATA Framework to over-ride the specific secrecy provisions that apply to the Time Capsule. Any attempt to use the DATA Framework to gain early access to Time Capsule data would represent an unacceptable risk to privacy, and a significant risk to the reputation of the Census. It may be sensible for the ABS to seek a specific exemption from the DATA Framework for the Time Capsule (if exemptions for specific datasets are available).	**Recommendation 14: Seek an exemption from the proposed DATA Framework for the Time Capsule** The ABS should seek an exemption for the Time Capsule from the proposed Data Availability & Transparency (DATA) Framework. This recommendation should be seen as the minimum ABS response to the proposed DATA framework, and not the full response.
F. Managing Function Creep **Inclusion of health data in the Time Capsule**	**Action Required**	A specific issue regarding the new collection of health information in the 2021 Census was raised by stakeholders. It was felt that the inclusion of this health information in the Time Capsule was high risk, as the Time Capsule is released as raw / identified data. Although Time Capsule data is not released until 99 years after it is collected, the inclusion of health information could have a potential impact on individuals. The presence of certain health conditions in individuals as revealed by the Time Capsule, might indicate the potential presence of genetically inherited conditions in their descendants. The data would be released with full names and would be searchable by members of the public. The health information might be a curiosity for future historians and family researchers, but it is not essential for it to be included in the Time Capsule. Removing the health data would reduce the overall security risk of the Time Capsule, as well as reducing any potential negative impacts from genetic profiling. Galexia is conscious that this recommendation may cause some communication challenges for the ABS (as it is obviously simpler to explain that all data is either in or out of the Time Capsule based on user choice). However, the data is simply too high a risk to be stored and then released in a raw / identified format.	**Recommendation 15: Remove the new health data collected in the 2021 Census from data submitted to the Time Capsule** The ABS should ensure that responses to the new long-term health conditions question are not included in the Time Capsule, and that this is clearly explained to consumers.

G. Reviewing the consequences for not responding to a Notice of Direction	**Action Required**	This PIA raises some concerns over the consequences for failing to respond to a Notice of Direction. Awareness of privacy, attitudes to data, and trust in government are all changing. The idea that an individual might end up with a criminal record for having strong concerns about privacy appears harsh, and the detriment to the overall Census may not justify the continuation of the traditional approach to prosecutions. This PIA includes a Recommendation for ABS to reform the refusals and prosecution process to implement a better balance between response rates and consequences for individuals facing prosecution.	**Recommendation 16: Review the consequences for refusing to complete the Census** The ABS should reform the refusals and prosecution process to implement a better balance between response rates and consequences for individuals facing prosecution. However, as it is unlikely that this issue can be resolved in time for the next Census, Galexia recommends that the proposed Census Privacy Strategy should include a review of the prosecution process for non-completion of the Census, and maximum penalty provisions (Refer to Structural Recommendation 1: Census Privacy Strategy).

23. Social Licence

One of the aims of the overall ABS Privacy Management Plan is to build a social licence for activities such as the 2021 Census.

A social licence is defined in the Productivity Commission Report on *Data Availability and Use* (2017)[57] as 'public trust, confidence and acceptance'. Although this definition is designed for data sharing, it applies fairly well to the Census, as Census data is also used in data linkage.

The Productivity Commission report suggested that it was important to develop public trust, confidence and acceptance (social licence) for data sharing. The report states that public trust and acceptance will develop if people:

- *have a sound basis for believing in the integrity and accountability of entities (public and private) handling data*
- *feel they have some control over how their own data is used and by whom, and an inalienable ability to choose to experience some of the benefits of these uses themselves*
- *better understand the potential community-wide benefits of data use.* (page 13)

In order to develop the social licence for the 2021 Census, ABS therefore needs to take measures to address each of these three components:

Social Licence Requirements	Action / Status	Galexia Commentary	Galexia Recommendation
A. A sound basis for believing in the integrity and accountability of the ABS	**Action Required**	Generally the ABS is a trusted and respected organisation. However, confidence in the Census was shaken by key events in relation to the 2016 Census, including: • The ABS decision to retain names and addresses indefinitely (later redacted to 4 years); • The ABS decision to conduct an internal PIA; • The conduct of a short public consultation period on the PIA during the Christmas holiday period; and • Interruptions to the Online Census service on Census night. It can be slow to repair an organisation's reputation. However the conduct of this independent PIA and the implementation of the recommended steps in this PIA (especially major changes such as reducing data retention periods) should help to restore community trust in the ABS. One major challenge for the Census is that key privacy stakeholders are rightly concerned at the lack of direct consultation with them over the content of the 2021 Census (which occurred prior to the commencement of this PIA).	This issue should be addressed by: • Structural Recommendation 1: Census Privacy Strategy; and • The two Recommendations on data retention: – Recommendation 5: Shorten data retention periods for names; and – Recommendation 6: Shorten data retention periods for addresses.

[57] Productivity Commission Inquiry Report, Australian Government, *Data Availability and Use* (2017) <www.pc.gov.au/inquiries/completed/data-access#report>.

B. Consumers feel they have some control over how their own data is used and by whom	**Action Required**	There are two key challenges in providing consumers with confidence over how their Census data is used: • **Data retention –** Names and addresses collected in the Census are currently held for too long. This undermines consumer confidence that their personal information is only being used for purposes that they understand and support, as it appears to set the stage for the long-term / indefinite retention of their data for unknown future purposes; and • **Data linkage –** The data linkage process is difficult for consumers to understand and there is a significant amount of incorrect information related to ABS data linkage processes in online commentary. It is hard to develop community confidence in the data linkage process in this environment.	Both of these issues should be addressed by: • Structural Recommendation 1: Census Privacy Strategy; • Structural Recommendation 2: Principles based approach to name encoding for data linkage; and • The two Recommendations on data retention: – Recommendation 5: Shorten data retention periods for names; and – Recommendation 6: Shorten data retention periods for addresses.
C. Consumers have the ability to choose to experience some of the benefits of data use themselves	**Compliant**	Consumers are likely to accept that some of the benefits of the Census are available for them to choose as individuals, such as data on education and transport.	–
D. Consumers understand the potential community-wide benefits of data use	**Compliant**	Consumers generally recognise the community-wide benefits of the Census, particularly in relation to the provision of government services and the management of elections. The inclusion of Indigenous data is also recognised as a significant community benefit.	–

24. Galexia Privacy Risk Identification

During the PIA process, Galexia has identified a number of privacy risks and graded these using Galexia's Privacy Risk Tool and ABS risk grading and scoring matrices. These have been grouped into themes and Galexia has proposed a number of treatments and mitigations to address each identified risk.

Galexia has summarised the risks below:

Summary of Risk Gradings by Privacy Risk Theme

Privacy Risk Summary	High	Medium	Low	Grand Total
Data minimisation		1		**1**
Data retention	1	1		**2**
Function creep	1	4		**5**
Governance	6	1		**7**
non-response			1	**1**
Openness	2			**2**
Re-identification		3		**3**
Reduced Trust		1		**1**
Security breach	6	1	1	**8**
Third party collection	2	1		**3**
Trigger questions		2		**2**
Grand Total	**18**	**15**	**2**	**35**

Summary Galexia Risk Assessment and mapping to Galexia PIA Recommendations

Candidate Risks developed by Galexia (as at April 2020)								
#	**Privacy Risk Theme**	**Risk event**	**Threat type**	**Likelihood**	**Consequence**	**Risk Event Rating**	**Risk Event Score**	**Recommendation / Actioned Mapping**
1	**Data minimisation**	Potential for all data subjects in Census data to be used in longitudinal studies.	**Compliance**	**Possible**	**Moderate**	**Medium**	**9**	Recommendation 10: Clarify the prohibition on using multiple Census collections in MADIP.
2	**Data retention**	Potential for citizens to be re-identified if address data is retained indefinitely.	**Compliance & Perception**	**Possible**	**Moderate**	**Medium**	**9**	Recommendation 6: Shorten data retention periods for addresses.
3	**Data retention**	Potential for citizens to be re-identified if name data is retained indefinitely.	**Compliance & Perception**	**Possible**	**Major**	**High**	**12**	Recommendation 5: Shorten data retention periods for names.
4	**Function creep**	Potential for a future Government to gradually allow the use of Census data for surveillance or compliance.	**Perception**	**Rare**	**Major**	**Medium**	**4**	Recommendation 12: Clarify ABS legislation to set out permitted and precluded purposes for use of Census data.

5	**Function creep**	Potential for a future Government to suddenly decide to use Census data for surveillance or compliance.	**Perception**	**Rare**	**Catastrophic**	**Medium**	**5**	Recommendation 12: Clarify ABS legislation to set out permitted and precluded purposes for use of Census data.
6	**Function creep**	Potential for future Governments to allow early access to some or all of the data in the Time Capsule.	**Perception**	**Unlikely**	**Major**	**Medium**	**8**	Recommendation 8: Clarify and strengthen access restrictions to data held in the Time Capsule.
7	**Function creep**	Potential for consumers to believe that responses to 'intrusive' questions may be used to find and target specific groups (e.g. Indigenous / veterans).	**Perception**	**Unlikely**	**Major**	**Medium**	**8**	Recommendation 12: Clarify ABS legislation to set out permitted and precluded purposes for use of Census data.
8	**Function creep**	Potential for data linkage (including Census) to become a platform for national surveillance or compliance.	**Perception**	**Possible**	**Major**	**High**	**12**	Recommendation 12: Clarify ABS legislation to set out permitted and precluded purposes for use of Census data.
9	**Governance**	Potential that the Census is not the correct vehicle to contain sensitive questions.	**Compliance**	**Likely**	**Minor**	**Medium**	**8**	Structural Recommendation 1: Census Privacy Strategy
10	**Governance**	Potential for ABS secrecy and confidentiality provisions to be 'trumped' by the proposed DATA Framework.	**Compliance & Perception**	**Possible**	**Major**	**High**	**12**	Recommendation 13: Clarify the relationship between Census data and the proposed Data Availability and Transparency Act (DATA) Framework.
11	**Governance**	Potential for the proposed DATA Framework to over-ride the specific secrecy provisions that apply to the Time Capsule.	**Compliance & Perception**	**Possible**	**Major**	**High**	**12**	Recommendation 14: Seek an exemption from the proposed DATA Framework for the Time Capsule.
12	**Governance**	Potential for a lack of privacy engagement during the development of Census questions.	**Compliance**	**Possible**	**Major**	**High**	**12**	Structural Recommendation 1: Census Privacy Strategy
13	**Governance**	Potential that the privacy rights are different online to that of paper.	**Compliance**	**Likely**	**Moderate**	**High**	**12**	Continue to review all Census contact points and privacy notices for consistency (Refer to APP 5. Notification issues resolved)
14	**Governance**	Potential for poor data quality if privacy concerns are heightened	**Compliance**	**Possible**	**Major**	**High**	**12**	Recommendations 5 & 6: Shorten data retention periods for names and addresses
15	**Governance**	Potential for Census data to be added to a large and ongoing national dataset, that is easily linked to named individuals.	**Compliance & Perception**	**Possible**	**Major**	**High**	**12**	Structural Recommendation 2: Principles based approach to name encoding for data linkage
16	**Non-response**	Potential for a backlash against the Census if individuals end up with a criminal record for attempting to exercise their right to privacy.	**Compliance & Perception**	**Rare**	**Minor**	**Low**	**2**	Recommendation 16: Review the consequences for refusing to complete the Census.
17	**Openness**	Potential for consumers to be unaware of, or confused by, the multiple pathways for Census data outputs.	**Compliance**	**Likely**	**Moderate**	**High**	**12**	Clarify Census 2021 data 'pathways' (Refer to APP 1. Privacy policy issues resolved)

18	Openness	Potential for ABS not to adequately disclose the consequences for individuals of not responding.	Compliance	Likely	Moderate	High	12	Recommendation 3: Clarify privacy notice information on the potential consequences for not providing information.
19	Re-identification	Potential for de-identified data to be re-identified in ACLD.	Compliance	Unlikely	Moderate	Medium	6	Recommendation 9: Conduct additional independent PIAs for activities that are 'renewed' for each Census
20	Re-identification	Potential for de-identified data to be re-identified in core Census products (e.g. TableBuilder).	Compliance	Unlikely	Major	Medium	8	Recommendation 4: Conduct independent security risk assessments for key 2021 Census components.
21	Re-identification	Potential for de-identified data to be re-identified in data integration projects.	Compliance	Unlikely	Major	Medium	8	Structural Recommendation 3: Principles based approach to managing re-identification risk
22	Reduced trust	Potential for reduced tolerance to sensitive questions.	Perception	Unlikely	Major	Medium	8	Recommendations 5 & 6: Shorten data retention periods for names and addresses
23	Security breach	Potential for security compromise via the MyWork App used by Census field staff.	Compliance	Unlikely	Minor	Low	4	Recommendation 17: Conduct an independent security review for the MyWork App.
24	Security breach	Potential for the cloud service provider (AWS) to access personal information.	Compliance & Perception	Unlikely	Moderate	Medium	6	Recommendation 4: Conduct independent security risk assessments for key 2021 Census components.
25	Security breach	Potential for security compromise of the identified data held in the Time Capsule.	Compliance & Perception	Unlikely	Catastrophic	High	10	Recommendation 9: Conduct additional independent PIAs for activities that are 'renewed' for each Census
26	Security breach	Potential for security compromise via remote access to Census data.	Compliance	Possible	Major	High	12	Recommendation 4: Conduct independent security risk assessments for key 2021 Census components.
27	Security breach	Potential for security compromise via insufficient vetting of researchers.	Compliance	Possible	Major	High	12	Structural Recommendation 3: Principles based approach to managing re-identification risk
28	Security breach	Potential for security compromise via the digital platform and / or cloud service provider.	Compliance	Possible	Major	High	12	Recommendation 4: Conduct independent security risk assessments for key 2021 Census components.
29	Security breach	Potential that the encoding algorithm is not strong enough to protect sensitive data.	Compliance & Perception	Possible	Major	High	12	Recommendation 4: Conduct independent security risk assessments for key 2021 Census components.
30	Security breach	Potential for security compromise via third party suppliers and contractors	Compliance	Possible	Major	High	12	Recommendation 11: Establish and maintain a register of third party agreements.
31	Third party collection	Potential for inclusion of health data (in the Time Capsule) to reveal genetic health information about future descendants.	Compliance & Perception	Likely	Minor	Medium	8	Recommendation 15: Remove the new health data collected in the 2021 Census from data submitted to the Time Capsule.
32	Third party collection	Potential for reliance on third party collection to be seen as privacy invasive.	Compliance	Likely	Moderate	High	12	Recommendation 2: Promote alternatives to third party collection.
33	Third party collection	Potential for the Census privacy notice to understate the extent of third party collection.	Compliance	Almost Certain	Moderate	High	15	Enhance privacy policy coverage of third party collection (Refer to APP 1. Privacy policy issues resolved)

34	**Trigger questions**	Potential for the question on the number of births to be seen as highly intrusive and in some cases to trigger a trauma response.	**Compliance & Perception**	**Possible**	**Moderate**	**Medium**	**9**	Structural Recommendation 1: Census Privacy Strategy
35	**Trigger questions**	Potential for the question on long-term health conditions (including a mental health condition response option) to be seen as highly intrusive and in some cases to trigger a trauma response.	**Compliance & Perception**	**Possible**	**Moderate**	**Medium**	**9**	Structural Recommendation 1: Census Privacy Strategy

ABS Risk Grading and Scoring Table

		Consequence				
		Insignificant	**Minor**	**Moderate**	**Major**	**Catastrophic**
Likelihood	**Almost Certain**	**Medium (5)**	**High (10)**	**High (15)**	**Extreme (20)**	**Extreme (25)**
	Likely	**Medium (4)**	**Medium (8)**	**High (12)**	**High (16)**	**Extreme (20)**
	Possible	**Low (3)**	**Medium (6)**	**Medium (9)**	**High (12)**	**High (15)**
	Unlikely	**Low (2)**	**Low (4)**	**Medium (6)**	**Medium (8)**	**High (10)**
	Rare	**Low (1)**	**Low (2)**	**Low (3)**	**Medium (4)**	**Medium (5)**

Appendices

Appendix A – Glossary and Acronyms

Acronym / Glossary	Description
ABS	Australian Bureau of Statistics <www.abs.gov.au>
ACLD	Australian Census Longitudinal Dataset <www.abs.gov.au/ausstats/abs@.nsf/mf/2080.0>. This dataset provides a longitudinal dataset covering multiple Censuses of a 5% random sample of data subjects.
ACMID	Australian Census and Migrants Integrated Dataset <www.abs.gov.au/ausstats/abs@.nsf/mf/3417.0.55.001>.
ACTEID	Australian Census and Temporary Entrants Integrated Dataset <www.abs.gov.au/AUSSTATS/abs@.nsf/Lookup/3419.0Main+Features12016>
APPs	Australian Privacy Principles <www.oaic.gov.au/privacy/australian-privacy-principles/>
ATO	Australian Taxation Office <www.ato.gov.au>
AWS	Amazon Web Services <www.aws.amazon.com>
CAT	Census Agent Tool
Census Number	A unique code used on letters and forms that links the letter or form to a target household address.
Census temporary password	Another unique code which is linked to the Census Number and is provided to enable login and completion of the Census online. Note: Users can also establish their own password.
CIAP	Census Independent Assurance Panel <www.abs.gov.au/websitedbs/d3310114.nsf/Home/Independent+Assurance+Panel>.
CSA	*Census and Statistics Act 1905 (Cth)*
DATA	*Data Availability and Transparency Act* (DATA) (proposed) <www.datacommissioner.gov.au/data-sharing/legislation>
DI	Data Integration
DIPA	Data Integration Partnership for Australia <www.pmc.gov.au/public-data/data-integration-partnership-australia>
DOB	Date of birth
EMI	Enumeration Management Information
EMS	Enumeration Management System
IT	Information Technology
IVR	Interactive Voice Response
LaM	Logistics and Materials team
Lossy (name) Encoding	Lossy encoding is an algorithm whereby many input values map to a single output (encoded) value. <www.ausstats.abs.gov.au/ausstats/subscriber.nsf/0/844269E83C4B6666CA25823C00178BBB/$File/1351055162_2018.pdf>
MADIP	Multi-Agency Data Integration Project <www.abs.gov.au/websitedbs/D3310114.nsf/home/Statistical+Data+Integration+-+MADIP>
MoU	Memorandum of Understanding
NAA	National Archives of Australia <www.naa.gov.au>
OAIC	Office of the Australian Information Commissioner <www.oaic.gov.au>
OVIC	Office of the Victorian Information Commissioner <www.ovic.vic.gov.au>
PI	Personal information
PIA	Privacy Impact Assessment <www.oaic.gov.au/privacy/guidance-and-advice/guide-to-undertaking-privacy-impact-assessments>
SI	Sensitive information

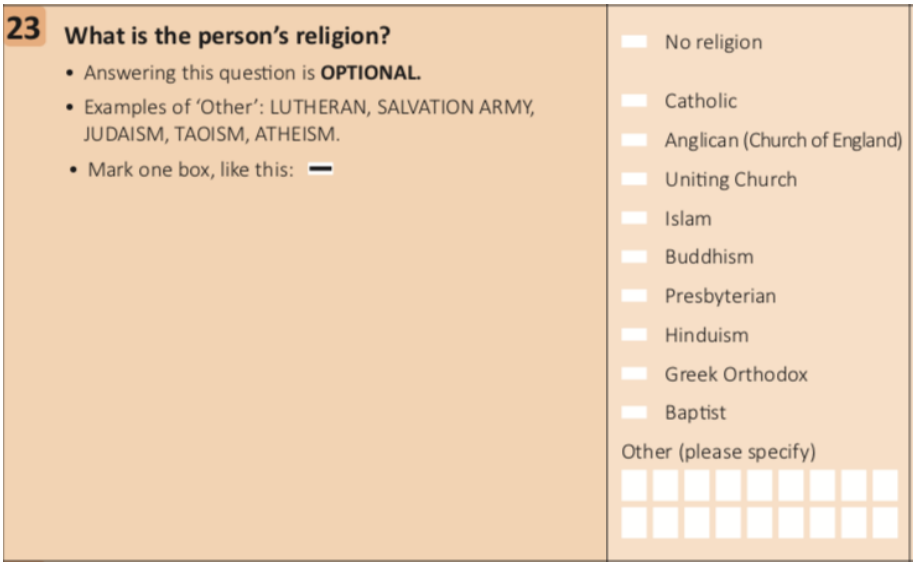
SLK	Statistical linkage key is a key that enables two or more records belonging to the same individual to be brought together. It is represented by a code consisting of the 2nd, 3rd and 5th characters of a person's family name, the 2nd and 3rd letters of the persons' given name, the day, month and year when the person was born and the sex of the person, concatenated in that order <www.abs.gov.au/AUSSTATS/abs@.nsf/lookup/4240.0.55.002Chapter15022011>.
TableBuilder	TableBuilder is a key data product which enables researchers to query underlying Census data online (for low risk data) or via a secure data lab (for higher risk data).
Time Capsule	The Time Capsule is a full copy of the Census forms completed by some individuals who have chosen to participate. It is stored by the National Archives of Australia and only released after 99 years.
WDB	Workgroup Database

Appendix B – Extracts from the Census Test Forms

The following extracts are from Census test forms. These were shared and discussed in Stakeholder forums.

2021 Census – Sample form – Questions 23, 28 & 51

Example 1: Optional question



23 What is the person's religion?

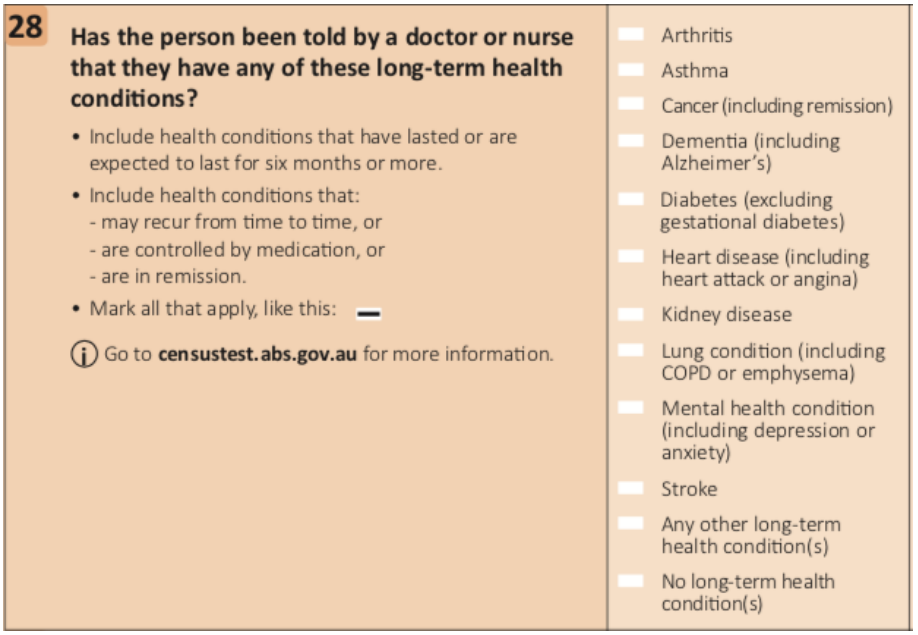
- Answering this question is **OPTIONAL.**
- Examples of 'Other': LUTHERAN, SALVATION ARMY, JUDAISM, TAOISM, ATHEISM.
- Mark one box, like this: —

- No religion
- Catholic
- Anglican (Church of England)
- Uniting Church
- Islam
- Buddhism
- Presbyterian
- Hinduism
- Greek Orthodox
- Baptist

Other (please specify)

Example 2: New question on long-term health conditions

Refer to Appendix F – Consultation Timeline on 2021 Census Topics for more detail on the consideration of the 'long-term health condition' topic.



28 Has the person been told by a doctor or nurse that they have any of these long-term health conditions?

- Include health conditions that have lasted or are expected to last for six months or more.
- Include health conditions that:
  - may recur from time to time, or
  - are controlled by medication, or
  - are in remission.
- Mark all that apply, like this: —

ⓘ Go to **censustest.abs.gov.au** for more information.

- Arthritis
- Asthma
- Cancer (including remission)
- Dementia (including Alzheimer's)
- Diabetes (excluding gestational diabetes)
- Heart disease (including heart attack or angina)
- Kidney disease
- Lung condition (including COPD or emphysema)
- Mental health condition (including depression or anxiety)
- Stroke
- Any other long-term health condition(s)
- No long-term health condition(s)

Example 3: New question on Defence Force service

51 **Has the person ever served in the Australian Defence Force?**

- Include Australian Army, Royal Australian Air Force, Royal Australian Navy, Second Australian Imperial Force, National Service and NORFORCE.
- Exclude service for non-Australian defence forces.
- Mark all that apply, like this: —

ⓘ Go to **censustest.abs.gov.au** for more information.

- No

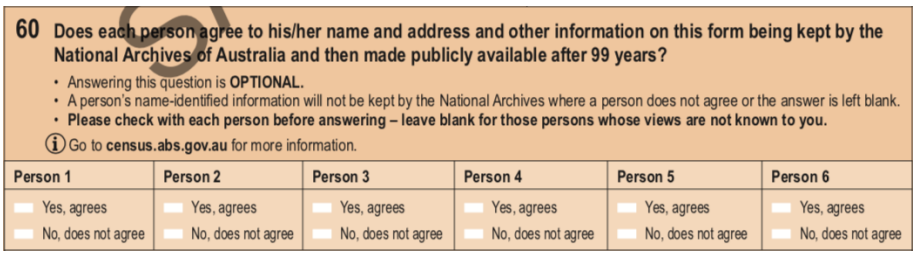
Regular Service

- Yes, current service
- Yes, previous service

Reserves Service

- Yes, current service
- Yes, previous service

2016 Census – Sample form – Question 60 (Time Capsule)



60 **Does each person agree to his/her name and address and other information on this form being kept by the National Archives of Australia and then made publicly available after 99 years?**

- Answering this question is **OPTIONAL.**
- A person's name-identified information will not be kept by the National Archives where a person does not agree or the answer is left blank.
- **Please check with each person before answering – leave blank for those persons whose views are not known to you.**

ⓘ Go to **census.abs.gov.au** for more information.

Person 1	Person 2	Person 3	Person 4	Person 5	Person 6
Yes, agrees	Yes, agrees	Yes, agrees	Yes, agrees	Yes, agrees	Yes, agrees
No, does not agree	No, does not agree	No, does not agree	No, does not agree	No, does not agree	No, does not agree

Appendix C – ABS 2021 Census Contact Points with the Public

The following table has been supplied by the ABS. It was prepared into an earlier recommendation (from the pre-PIA Report[58]) that the ABS should review all contact points and ensure a consistent privacy message was being delivered.

Contact Points with public	How we notify the public of the Collection Notice/Privacy Policy/about their PI	PI Information we collect
ABS and Census Websites • Online completion of Census eForm • Web based self-service and 'Contact Us' forms • Visiting Privacy Policy on Census page	• Stated at start of Census online form with link to privacy policy online • Link to privacy policy from Census page	• **Census form:** all PI/SI • Name, • Address, • Census Number
Mainstream Enumeration • Field Manager (FM) • Mobile Field Rep (MFR) • Field Officer (FO) • Establishment Officer (EO)	• Face to face advice to go to website • Stated on hardcopy form • Refer to ABS website for the collection notice/privacy policy	• Name • Address • Comments
Remote Operations • Census Operations Manager • Assistant Operations Manager • Remote Area Management Team Leader • Remote Area Management Team Member • Community Field Officer • Establishment Officer	• Face to face advice to go to website • Stated on hardcopy form	• **Census form:** all PI/SI
Assisted Completion • Census Engagement Manager • Assistant Engagement Manager • Local Engagement Officer • Community Field Office	• Face to face advice to go to website • Stated on hardcopy form	• **Census form:** all PI/SI
Face to face service point • Census Engagement Manager • Assistant Engagement Manager • Local Engagement Officer • Community Field Office	• Face to face advice to go to website • Stated on hardcopy form	• Name • Address
Contact Centre: • Services Australia & ABS Automated Paper Form Request Service	• Stated in the recording message • Refer to website for policy • Press 1 to listen to Privacy Policy	• Name • Address • Comments
Guided Chatbot	• Link to Privacy Policy online	[None collected]
Letter/email	• State in response letter to go to website to view Privacy Policy	• Name • Address • Email • Phone number

[58] EY, *Pre-PIA Review*, Census 2021 (11 September 2019) [internal document]

Appendix D – Stakeholders and Meetings

Galexia met with a wide range of internal and key external stakeholders during the development of this PIA. We also offered consultations to a wider group of stakeholders, although not everyone was able to participate.

External Stakeholders

Galexia met with key external stakeholders at an early stage of the PIA process, and then contacted them again later in the process to 'bench test' a selection of the most significant PIA Recommendations.

The consultation process concentrated on civil society advocates and privacy regulators as well as key academics who worked on issues related to de-identification and re-identification risk.

The following organisations participated in consultations during this PIA:

- **Privacy regulators:**
  - Office of the Australian Information Commissioner (OAIC) <www.oaic.gov.au>
  - Office of the Victorian Information Commissioner (OVIC) <www.ovic.vic.gov.au>
- **Academics:**
  - Macquarie University
  - University of Melbourne
- **Civil society advocates:**
  - Australian Communications Consumers Action Network (ACCAN) <accan.org.au>
  - Australian Council of Social Services (ACOSS) <www.acoss.org.au>
  - Australian Privacy Foundation (APF) <www.privacy.org.au>
  - Consumers' Health Forum (CHF)) <chf.org.au/>
  - Electronic Frontiers Australia (EFA) <www.efa.org.au>
  - Liberty Victoria <libertyvictoria.org.au>

The initial round of consultations helped inform the development of key recommendations, particularly the three Structural Recommendations. Galexia heard significant concerns (and some confusion) around the ABS processes for name encoding, data integration and data de-identification. Stakeholders also raised concerns about the following issues:

- Civil society stakeholders raised concerns about their exclusion from the process for developing new Census questions, particularly where they had a high privacy impact (such as the new question on long-term health conditions);
- Academic stakeholders raised potential issues related to re-identification risk; and
- Privacy regulators shared many of these concerns, but also queried the potential impact of the DATA Framework on the privacy arrangements for future Censuses.

In February 2020 Galexia re-contacted stakeholders to 'bench test' their views on the three proposed Structural Recommendations and some selected key recommendations. Stakeholder responses are summarised in the following table (note that no responses were received from academic stakeholders):

Recommendation	Advocates	Regulators
Structural Recommendation 1: Census Privacy Strategy	Supported or supported in principle	Generally supportive
Structural Recommendation 2: Principles based approach to name encoding for data linkage	Some support, but advocates believe the principles may not provide enough protection. They also argued that the data minimisation principle should also apply to name and address retention.	Generally supportive

Structural Recommendation 3: Principles based approach to managing re-identification risk	Some support, but reliance on legal agreements was seen as unwise. They also suggested the exception mechanisms must be subject to independent oversight. Their biggest concern was the initial decision to rely on names and addresses.	Generally supportive. The OAIC also pointed to guidance in the Data61 /OAIC De-Identification Decision-Making Framework.[59]
Recommendation 2: Promote alternatives to third party collection	Some support, but advocates were disappointed that topics and questions are not within scope of the PIA.	Generally supportive
Recommendation 5: Shorten data retention periods for names and **Recommendation 6:** Shorten data retention periods for addresses	Some support, but concerned with the initial decision to rely on names and addresses.	Generally supportive
Recommendation 12: Clarify ABS legislation to set out permitted and precluded purposes for use of Census data	Supported	Support for provisions to be prescribed in primary legislation
Recommendation 14: Seek an exemption from the proposed DATA Framework for the Time Capsule	This position was not supported by advocates. They did not believe the wording: 'should consider' is strong enough language.	Support for ABS to develop a clear position and approach.
Recommendation 15: Remove the new health data collected in the 2021 Census from data submitted to the Time Capsule	Supported	Support for ABS to develop a clear position and approach.
Recommendation 16: Review the consequences for refusing to complete the Census	Supported	Generally supportive

[59] *De-identification Decision-Making Framework*, Office of the Australian Information Commissioner (OAIC) and Data61 (CSIRO), September 2017 <www.oaic.gov.au/privacy/guidance-and-advice/de-identification-decision-making-framework>.

ABS Internal stakeholder meetings

Galexia also held extensive meetings with ABS internal teams and senior management. Galexia was provided with unlimited access to ABS staff and contractors, and we met with some teams on multiple occasions. The ABS supplied over 100 documents and information resources to assist in the preparation of the PIA.

ABS internal stakeholders that participated in the PIA process included:

1) 2021 Census Privacy Team
2) Statistical Data Integration Division
3) 2021 Census Executive
4) Data Operations
5) 2021 Census Field Operations
6) Information Technology
7) 2021 Census Contact Centre
8) 2021 Census HR and Adecco
9) 2021 Census Content and Dissemination
10) 2021 Census Enumeration
11) 2021 Census Field Operations Management and Training
12) 2021 Census Digital and Paper Service
13) ABS HR and Adecco
14) 2021 Census Inclusive Strategies
15) ABS Privacy Team
16) ABS Privacy Champion
17) Data Linkage
18) Data Integration and Access Support
19) Customised and Microdata Delivery
20) MADIP
21) Deputy Australian Statistician, Census & Data Services Group
22) 2021 Census Data Operations
23) Data Integration Delivery Assurance and Strategy
24) 2021 Census Refusals Team
25) 2021 Census Content
26) General Manager, Census Division
27) MyWork App
28) Risk, Planning & Policy Branch and Privacy Officer
29) Australian Statistician
30) General Manager, Statistical Data Integration Division
31) Chief Methodologist

Appendix E – Employee Data

The proposed design of the 2021 Census has delivered a mix of privacy strengths and weaknesses in relation to employee data.

Strengths

- The ABS has strong HR systems and security in place;
- The ABS has comprehensive privacy training in place for new and existing staff;
- The ABS is making good progress on developing an overall 'privacy culture', with strong leadership from the Privacy Champion and dedicated privacy teams;
- Clear identification of field staff is in place, including communications with police and local communities about how to identify authentic Census field staff;
- The third party agreement with Adecco includes comprehensive privacy and security measures; and
- ABS staff have access to privacy scripts and documentation that 'anticipate' most privacy issues and concerns.

Weaknesses

- There are likely to be some privacy challenges in managing all aspects of remote working; and
- The sheer scale and temporary nature of the workforce may increase privacy and security risks (the ABS engages around 30,000 temporary staff in order to conduct the Census).

The following chart summarises the key information flows for Census employees:

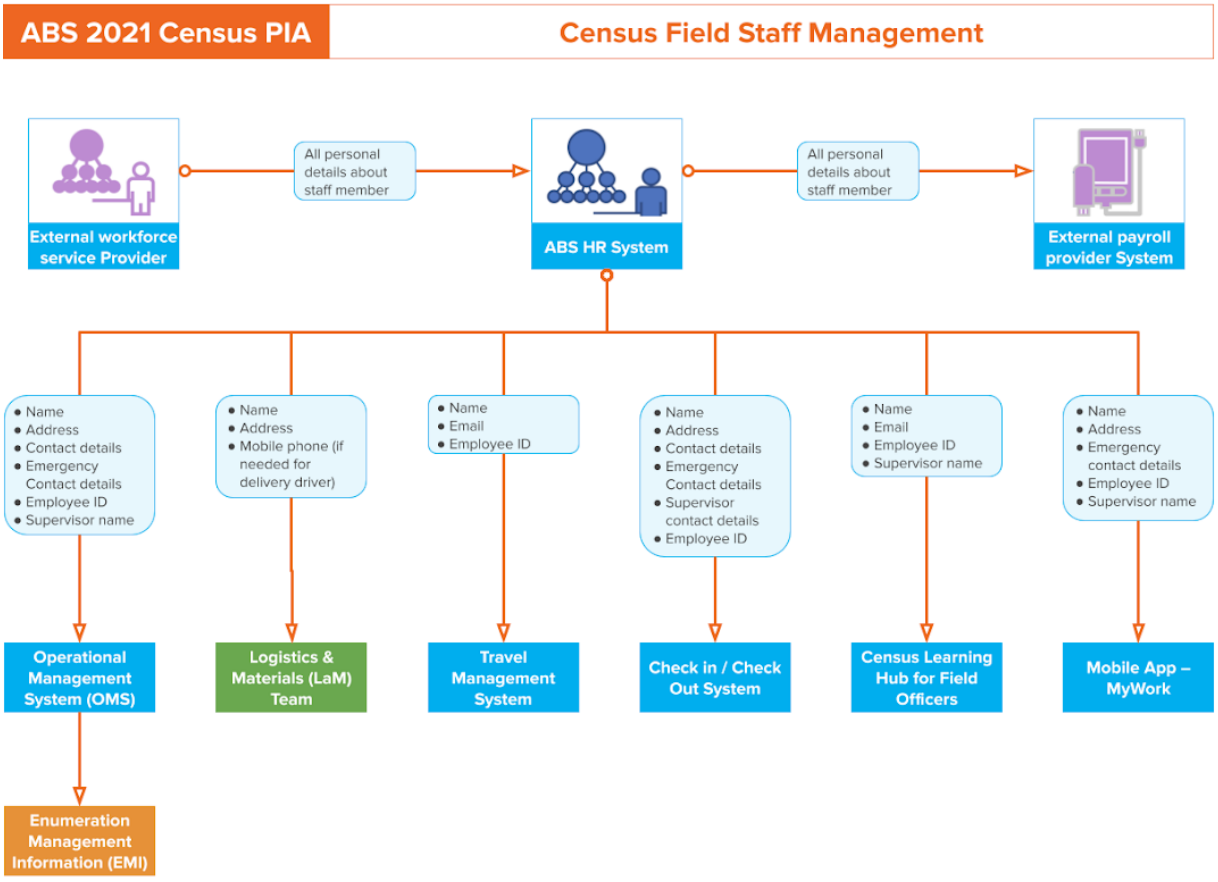


Diagram: Census Personal / Sensitive Information Flow – Census Field Staff Management – April 2020 (information supplied by ABS)

This PIA briefly assessed the proposed 2021 Census arrangements for employee data against the APPs.

The following table summarises the main findings:

Australian Privacy Principle (APP)	Action / Status	Galexia Commentary	Galexia Recommendation
APP 1 – Openness and Transparency	**In progress**	The ABS maintains a public privacy policy that is specific to employees: **ABS Recruitment Privacy Statement[60]** This policy is the subject of a current review (along with all ABS privacy policies). At the time of completing this PIA in April 2020, the policy was generally accurate and compliant with APP 1, but the review may result in some minor changes and updates. For example, the names and contact details of key third party providers involved in the recruitment process may be added to the policy. The general ABS Privacy Policy[61] also applies to ABS employees (for example where the employee privacy policy is silent on an issue, such as access and correction rights). This is noted in the employee privacy policy and a link to the main policy is provided. For the Census, ABS is partnering with the Adecco Group <www.adecco.com.au> to help manage the large workforce required for specific Census tasks.[62] **Adecco Group Privacy Information Statement[63]** The Adecco group privacy policy / privacy information statement is accurate and up to date, and fully complies with APP 1. **Adecco Data Protection Policy[64]** Adecco also has a formal Data Protection Policy (2018) in place. This is similar to a Privacy Management Plan and includes an overall strategy for managing privacy and promoting Privacy by Design in Adecco projects.	–
APP 2 – Anonymity and Pseudonymity	**Compliant**	The anonymity principle is not particularly relevant to employees, although members of the public can generally browse ABS job opportunities without registering any personal details.	–

[60] ABS, *Recruitment Privacy Statement* (14 November 2018) <abs.gov.au/websitedbs/corporate.nsf/home/Privacy+Statement>.

[61] ABS, *Privacy Policy* (6 January 2020) <www.abs.gov.au/websitedbs/D3310114.nsf/Home/Privacy+Policy>.

[62] ABS, *Media Release: ABS appoints PwC Australia and The Adecco Group Australia to deliver key 2021 Census services* (3 May 2019) <www.abs.gov.au/ausstats/abs%40.nsf/mediareleasesbyCatalogue/4D95297065D18DA2CA2583EE0080A857>

[63] Adecco Group, *Privacy Information Statement* (v4 of 1 April 2020) <www.adecco.com.au/media/adecco-au/privacy-policy/Adecco-Group-Privacy-Policy.pdf>

[64] Adecco Group, *Data Protection Policy* (GP 01.13/002 of 18 April 2018) [Internal document]

APP 3 – Collection of solicited personal information	**Compliant**	The ABS employment process for the Census follows standard ABS practices. Only relevant information is collected (in compliance with the data minimisation principles in APP 3), and most information is collected directly from the employee. Some third party checks are carried out, but these are consistent with the expectations of employees and are acceptable under APP 3. These include: ● Criminal record checks; ● References; and ● Information from recruiters (supplied with employee consent). Some sensitive information is collected on health and accessibility issues, usually to manage access issues for employees (and prospective employees who may need assistance for interviews). This information is collected with the consent of the individual.	–
APP 4 – Dealing with unsolicited personal information	**Compliant**	APP 4 is not particularly relevant to employees.	–
APP 5 – Notification	**Compliant**	The ABS recruitment process does not include a specific short form privacy notice. Instead all recruitment forms have a direct link to the full **ABS Recruitment Privacy Statement.**[65] That statement complies with APP 5, and includes a further link to the main ABS Privacy Policy for further information.	–
APP 6 – Use or Disclosure	**Compliant**	The use of employee data in the Census process is dependent on the type of employee: ● ABS core Census team; ● Census field workers; ● Census Contact Centre staff; and ● Temporary Census staff. Some typical employment related disclosures of information are flagged in the ABS and Adecco privacy policies. These include disclosures to: ● Workers Compensation bodies; ● Employers seeking references; and ● Training, education and qualifications providers. All of the proposed disclosures are compliant with APP 6.	–
APP 7 – Direct Marketing	**Compliant**	This APP is not particularly relevant to employees. Some personal contact details of former employees may be used in order to inform ex-staff and / or unsuccessful job applicants about future work opportunities. These opportunities may be within the ABS or other Commonwealth agencies. However, employees must register for this service and provide their consent. The program is fully described in the ABS Recruitment Privacy Statement. This use is within the expectations of employees, and individuals can easily have their details removed.	–

[65] ABS, *Recruitment Privacy Statement* (14 November 2018) <abs.gov.au/websitedbs/corporate.nsf/home/Privacy+Statement>.

APP 8 – Cross-border Disclosure	**Compliant**	Employee data is maintained in Australia. For the Census, ABS is partnering with the Adecco Group to help manage the large workforce required for specific Census tasks. Cross-border data transfers are prohibited in the agreement between ABS and Adecco.	–
APP 9 – Government Related Identifiers	**Compliant**	ABS, Adecco and EPI-USE (the payroll provider) collect and use a range of identifiers in order to facilitate the employment process. These include: • **Tax File Numbers (TFNs)** These are used to manage payroll and their collection and use is authorised by legislation; • **Driver Licence Numbers** These are used and checked where field workers are required to drive (usually in their own vehicle) as part of Census field work; and • **Australian Public Service (APS) numbers** These are created, used and disclosed in accordance with whole of government arrangements for Commonwealth employees. None of these uses create issues under APP 9 as this APP is really targeted at the creation of a new identifier or the use of existing identifiers by the private sector. Although the Adecco group is a private sector organisation, for the purposes of the Census it is a Commonwealth contractor and is not impacted by APP 9, as long as it returns employee data to the ABS once the contract is completed.	–
APP 10 – Quality of Personal Information	**Compliant**	This PIA has not considered data quality issues in detail in relation to Census employees, but no issues have been identified.	–
APP 11 – Security	**In progress**	For the Census, ABS is partnering with the Adecco Group to help manage the large workforce required for specific Census tasks. **General security** The agreement with Adecco includes extensive security requirements relating to IT security, physical security, data breaches and requires the return of ABS information at the conclusion of the contract. Adecco also developed a formal security incident response plan for the Census test in 2019, which can be extended to the full Census in 2021.[66] **App security** The ABS has developed a specific App for use by Census staff – the MyWork App. The App helps field staff to manage their tasks and time, and provides a simple way of connecting to core ABS systems and updating progress. The MyWork App collects and shares some employee data, including potential information on location and movements. The App should be the subject of an independent security review, as Apps are often a weak point in security arrangements. This is because they have to operate on a wide variety of devices and operating systems, and the devices are not in the direct control of the ABS at all times.	**Recommendation 17: Conduct an Independent security review for the MyWork App** The ABS should commission an independent security risk assessment for the proposed MyWork App. **Note:** This review will be scheduled by the ABS

[66] Adecco Group, *Security Incident Response Plan for Third Parties (2019 Census Test)* (5 August 2019) [Internal document]

APP 12 – Access	**Compliant**	The general ABS Privacy Policy includes a small section on access rights. Although the ABS has a general exception to APP 12 available for statistical information (e.g. Census content), this exception does not apply to employee data. The ABS complies with APP 12 for employee requests.	–
APP 13 – Correction	**Compliant**	The ABS complies with APP 13 in relation to employee complaints.	–

Appendix F – Consultation Timeline on 2021 Census Topics

- **Late 2017** – ABS consulted with key users of Census data about changes or additions.
- **3 Apr 2018** – Consultation on Topics announced by Australian Statistician.[67]
    - Refer to reference to 'Health' under *Other Topics.*[68]
- **Apr-Jun 2018** – Formal ABS consultation process on the 2021 Census topics.[69]
    - 450 submissions were received on topics and 315 published.[70]
    - Galexia's analysis of the 315 published submissions:
        - There were **two** submission that referred to privacy – and these were with reference to new topics where existing privacy laws were seen as a blocker;
        - There were **no** submissions from civil society, consumer or privacy advocates about the privacy aspects of topics and questions.
- **14 Nov 2018** – Media Release: *ABS tests topics for 2021 Census to reflect changing nation*[71]
    - Refer to *Topic Directions: Health*[72]

> *Currently, there are no questions regarding health asked in the Census, but for some years health topics have been of interest to stakeholders.*
>
> *CHRONIC HEALTH CONDITIONS*
>
> *There was strong support through consultations and from submissions outlining a need for data on the health status of Australians, with particular interest in being able to analyse data on chronic health conditions against geographic and socio-economic variables.*
>
> *Stakeholders supported the inclusion of a new chronic health conditions topic (this term was used interchangeably with 'long term health conditions'). Further engagement with stakeholders and testing will refine data needs and identify the health conditions that could be included in a Census question.*

- **Oct-Nov 2019** – Galexia shared a proposed new question on long-term health conditions (Q28) and Defence Force service (Q51) with external stakeholders. This was the first time these questions had been considered by privacy and consumer advocates. Refer to Appendix B – Extracts from the Census Test Forms.
- **13 Dec 2019-10 Jan 2020** – Treasury Consultation on *Census and Statistics Amendment (Statistical Information) Regulations 2019*[73] for the purpose of adding *'Australian Defence Force service and chronic illness to the list of topics'.*
    - The detail in the Exposure Draft and Explanatory Statement was sparse:

> *Item 2 inserts a topic relating to health conditions diagnosed by a doctor or a nurse. This topic will be answered by all respondents and assist health service planning and service delivery at the local level.*

    - Submissions to Treasury have not been made available.

[67] <abs.gov.au/ausstats/abs@.nsf/mf/2007.0>

[68] <www.abs.gov.au/ausstats/abs@.nsf/Lookup/by%20Subject/2007.0~2021~Main%20Features~Other%20topics~18>

[69] <consult.abs.gov.au/census/census-topics>

[70] <consult.abs.gov.au/census/census-topics/consultation/published_select_respondent>

[71] <www.abs.gov.au/ausstats/abs@.nsf/Lookup/by%20Subject/2007.0.55.001~2021~Media%20Release~ABS%20tests%20topics%20for%202021%20Census%20%20(Media%20Release)~10000>

[72] <www.abs.gov.au/ausstats/abs@.nsf/Lookup/by%20Subject/2007.0.55.001~2021~Main%20Features~Health~18>

[73] <treasury.gov.au/consultation/c2019-41183>

- **6 Feb 2020** – *Census and Statistics Amendment (Statistical Information) Regulations 2020* enacted.[74]

  > *EXPLANATORY STATEMENT*
  >
  > *ATTACHMENT B*
  >
  > *The Regulations engage a person's right to privacy as they require the Statistician to collect personal information about respondents' Australian Defence Force service and diagnosed health conditions.*
  >
  > *….the Regulations impose a permissible limitation on the protection against interference with the right to privacy.*

- **12 February 2020** – ABS publicly released the proposed new long-term health conditions and Defence Force service question in *ABS Review of 2021 Census Topics.*[75]

[74] <www.legislation.gov.au/Details/F2020L00109>

[75] <www.abs.gov.au/websitedbs/D3310114.nsf/Home/2021+Census+review+of+topics>