Australian Bureau of Statistics

Canberra Office
ABS House
45 Benjamin Way
Belconnen ACT 2617
Phone 1300 135 070

Locked Bag 10
Belconnen ACT 2616

www.abs.gov.au
ABN 26 331 428 522

Privacy Impact Assessment:

Proposal to Retain Name and Address Information from Responses to the 2016 Census of Population and Housing

December 2015

Contents

Executive Summary 3
1. Introduction 5
1.1. Project Overview 5
1.2. Privacy Impact Assessment Methodology 5
2. Project Description 6
2.1. Background and Rationale 6
2.2. Legal Authority 8
2.3. Governance and Institutional Arrangements 9
2.4. Retention and Use of Information 11
2.5. Information Flows 12
2.6. Security of Information 16
2.7. Disclosure of Information 18
2.8. Access to and Correction of Information 18
3. Stakeholder Consultation 19
4. Privacy Risk and Mitigation 21
4.1. RISK: Unauthorised access by ABS staff to data stored in the ABS environment 21
4.2. RISK: Unauthorised non-ABS access to data stored in the ABS environment 21
4.3. RISK: Accidental release of name and/or address data in ABS outputs or through loss of work related IT equipment and IT documentation 22
4.4. RISK: Reduction in participation levels in ABS collections due to loss of public trust 23
4.5. RISK: 'Function creep' – unintentional expanded future use of retained name and address information 23
5. Conclusion 25
Recommendations 25
Appendix A – Media Release 26
Appendix B – Statement of Intent 27

Executive Summary

The Australian Census of Population and Housing (Census) collects information relating to each person and household in Australia. While the Census collects information about each person and household, it is not concerned with information about individuals as such. The Census is conducted to provide information about the community as a whole and about groups within the community. The public expects that the information they provide to the ABS will be kept confidential.

The retention of names and addresses from responses to the 2016 Census would support ABS' ability to provide a richer and dynamic statistical picture of Australia through the integration of Census data with other survey and administrative data, the geospatial enablement of that data, and improvements to our household surveys. The retention of names and addresses would also reduce the cost to taxpayers and the burden on Australian households through more efficient ABS survey operations.

Under this proposal, names and addresses would be stored separately from other household and person data collected in the Census. Names and addresses would also be stored separately from each other. Addresses and anonymised versions of names would only be used for projects approved by a senior-level committee, and would be subject to strict information security provisions.

The ABS is committed to maintaining the highest levels of community trust and meeting its legislative obligations. There would be no change to existing ABS practices and obligations that ensure that no information is released in a way that would enable users of Census data to identify any particular individual or household. This includes names and addresses.

Consistent with best practice, the ABS has undertaken a Privacy Impact Assessment to identify the risks that the retention of names and addresses from responses to the 2016 Census might have to the privacy of individuals, and to assess the ABS' proposed approach to managing, minimising or eliminating those risks. The Privacy Impact Assessment has been undertaken in accordance with the framework for Privacy Impact Assessments set out in the Office of the Australian Information Commissioner's *Guide to undertaking Privacy Impact Assessments*. The ABS also referred to the Office of the Australian Information Commissioner's *Guide to information security* and *Guide to handling personal information security breaches*.

The outcome of the Privacy Impact Assessment has determined that the retention of names and addresses from responses to the 2016 Census is consistent with the functions of the ABS prescribed in the *Australian Bureau of Statistics Act 1975* and compliant with all the provisions in the *Census and Statistics Act 1905* and the *Privacy Act 1988*, including the Australian Privacy Principles.

The Privacy Impact Assessment identified a small number of potential risks to personal privacy associated with the retention of names and addresses from responses to the 2016 Census, but concluded that in each case the likelihood of these risks eventuating was 'very low'. The Privacy Impact Assessment determined that these risks can and would be effectively mitigated by implementation of an internationally accepted practice known as functional separation and by existing ABS governance and security arrangements. Nevertheless, a small number of recommendations have been made in relation to implementation of the proposal.

The outcome of this Privacy Impact Assessment, along with feedback from key stakeholders and the public, will inform the ABS' decision to retain names and addresses from responses to the 2016 Census. The ABS will publish its decision and this Privacy Impact Assessment on the ABS website by the end of 2015.

1. Introduction

1.1. Project Overview

The Australian Bureau of Statistics (ABS) is conducting this Privacy Impact Assessment on the retention of names and addresses collected in the 2016 Census of Population and Housing (Census). The retention of names and addresses from responses to the 2016 Census would enable the ABS to deliver richer statistics and increase the value of existing data to better inform planning decisions and government policies for a better Australia. Section 2.1 provides more information on the public benefits of this proposal.

Historically, the ABS has destroyed name and address information after statistical processing of the Census has been completed.[1] The ABS is now considering the retention of names and addresses from the 2016 Census as a key enabler to meet the growing stakeholder demand to provide a richer and more dynamic statistical picture of Australia through the integration of Census data with other survey and administrative data, the geospatial enablement of that data, and improvements to our household surveys. The retention of names and addresses would also reduce the cost to taxpayers and the burden on Australian households through more efficient ABS survey operations

In considering this change, the ABS remains committed to maintaining the highest levels of community trust and meeting its legislative obligations. The proposal to retain names and addresses from responses to the Census is made in accordance with the provisions for protecting personal privacy in the *Census and Statistics Act 1905* (Cth) and the *Privacy Act 1988* (Cth), including the Australian Privacy Principles. No change is proposed to ABS' existing practices and obligations to ensure that no information is released by the ABS in a way that would enable users of Census data to identify any particular individual or household.

The proposal is for names and addresses to be stored separately from other household and person data collected in the Census. The names and addresses themselves would also be stored separately from each other. Only anonymised versions of names would be used for projects that are both approved by a senior-level committee and subject to strict security provisions.

To inform the ABS' decision and approach, the ABS has undertaken this Privacy Impact Assessment and has sought feedback on this proposal. A Media Release and Statement of Intent were released by the ABS on 11 November 2015. Feedback on the proposal was sought by 2 December 2015. Stakeholder feedback has been considered in finalising this Assessment.

1.2. Privacy Impact Assessment Methodology

Australian Privacy Principle 1 requires Australian Privacy Principle entities to take reasonable steps to implement practices, procedures and systems that will ensure compliance with the Australian Privacy Principles and enable them to deal with enquiries or complaints about privacy compliance. In this way, the Australian Privacy Principles require 'privacy by design', an approach whereby privacy

[1] Currently, the ABS destroys all name-identified Census information after statistical processing except where people have explicitly consented to their personal information being retained for 99 years by the National Archives of Australia as part of the Census Time Capsule. The ABS proposal to retain name and address information from responses to the 2016 Census is independent of the Census Time Capsule scheme.

compliance is designed into projects dealing with personal information right from the start, rather than being bolted on afterwards.

As detailed below, the ABS has established governance systems consistent with Australian Privacy Principle 1.

In the interests of transparency, the ABS has undertaken this Privacy Impact Assessment to identify the risks that the proposal to retain names and addresses from responses to the Census might have on the privacy of individuals, and to assess the ABS' proposed approach to managing, minimising or eliminating those risks. This Privacy Impact Assessment has been undertaken in accordance with the framework for Privacy Impact Assessments set out in the Office of the Australian Information Commissioner's *Guide to undertaking Privacy Impact Assessments*[2]. The ABS has also referred to Office of the Australian Information Commissioner's *Guide to information security*[3] and *Guide to handling personal information security breaches*[4].

As a part of the decision making process on whether to adopt the proposal, feedback has been sought directly from Commonwealth, State and Territory Information and/or Privacy Commissioners, or relevant representatives. Feedback has also been sought from the public via a media release and Statement of Intent published on the ABS website. See Appendix A for the Media Release and Appendix B for the Statement of Intent.

The ABS will review the outcomes of this Privacy Impact Assessment and take into consideration all feedback received to decide whether to proceed with the proposal to retain names and address from responses to the 2016 Census.

2. Project Description

2.1. Background and Rationale

Australia's seventeenth national Census will be held on Tuesday, 9 August 2016. The Census provides a comprehensive picture of Australia in order to inform decision-making, policy development, and the provision of funding and services by governments and other users.

The ABS has four goals for the 2016 Census. These are to:

1. count every dwelling and person in Australia on Census night;
2. maximise the value of Census data to all users;
3. protect the privacy of the public; and
4. increase the efficiency and sustainability of the Census.

[2] Office of the Australian Information Commissioner (May 2014), *Guide to undertaking privacy impact assessments.*
[3] Office of the Australian Information Commissioner (August 2014), *Guide to information security*.
[4] Office of the Australian Information Commissioner (August 2014), *Guide to handling personal information security breaches*.

Consistent with these goals, the 2016 Census will be a launching pad for a transformation of the way the ABS collects and provides access to data about Australia's population. The ABS aims to move to an integrated approach to the collection and compilation of data from existing datasets.

The 2016 Census also provides an opportunity to improve and expand the information available to Australians through the ABS Census Data Enhancement program[5]. This program uses statistical data integration techniques to bring together 2016 Census data with previous Censuses (2006 and 2011) and other survey and administrative datasets.

Together these initiatives would continue to provide new statistical and analytical insights and ensure that the Census delivers maximum benefit to governments and the community. As part of this transformation, the ABS is exploring the retention of names and addresses from responses to the 2016 Census to provide a benefit to the ABS and wider community by:

- enabling higher quality and more efficient linkage of high value survey and administrative datasets with the Census, particularly for small or highly mobile sub-populations of policy interest;
- supporting a range of organisational efficiencies, such as the development of an address register, improving sampling, imputation and provider management; and
- supporting more flexible geospatial outputs.

More specifically, the use of statistical data integration techniques to bring together Census data with other survey and administrative data would enable the ABS to meet the growing demand of policy agencies (e.g. Department of Social Services, Department of Health), service providers and the research community for higher quality 'joined-up' information to better inform planning decisions and government policies in the public good. In particular, the use of names and addresses to improve the quality and accuracy of linked information, would enhance the ability of policy makers and researchers to effectively measure changes over time or differences between population sub groups or regions.

Bringing Census data together with education and health data, for example, can provide insight into, and help improve education, employment and health systems and services and can help answer questions such as:

- what is the impact of early childhood experiences on successful transition to school and longer term outcomes?
- how could education approaches be improved across the lifecycle to help young adults achieve higher levels of employment?
- what factors matter for targeting health services for those most in need, including mental health services? How could these insights assist with the design of better programs of support and prevention?

[5] The ABS Census Data Enhancement Program commenced with the 2006 Census. The Program brings together Census data with other data sources to inform key policy and research questions. The Program continued with the 2011 Census and an overview of outcomes from the 2011 Census can be found in *Census Data Enhancement project: An update, 2011, ABS cat. No. 2062.0.*

- what are the outcomes for individuals and families who receive assistance from a range of social services – child care, housing and homelessness services, child protection services, disability services, etc?
- do young unemployed adults move to areas of higher employment? For those that move, do they have better or worse outcomes than those who don't?
- what is the impact of industry restructuring (e.g. the automotive industry) on community and individual outcomes?

In considering this proposal to retain names and addresses from the 2016 Census, the ABS remains committed to maintaining the highest levels of community trust. The ABS would apply well established and internationally accepted separation principles to protect privacy and data. These principles essentially separate data items into different data stores. The ABS proposes to store names and addresses separately and securely from other household and personal data collected in the Census. The proposal would be to also store names and addresses separately from each other. Addresses and anonymised versions of names would only be used for approved projects which are also subject to strict security provisions.

The ABS is proposing no change to our practice and legal obligation to ensure that no information would be released by the ABS in a way that would enable users of Census data to identify any particular individual or household.

This Privacy Impact Assessment ensures that appropriate identification and assessment of risks has been undertaken, and that appropriate controls are in place or can be implemented to mitigate risks.

A decision on whether to proceed with the proposal to retain name and address information from responses to the 2016 Census, informed by this Privacy Impact Assessment and stakeholder feedback, will be made and the outcome published by the end of 2015.

2.2. Legal Authority

The *Australian Bureau of Statistics Act 1975* (Cth) and the *Census and Statistics Act 1905* (Cth) set out the primary functions, duties and powers of the ABS. The ABS is also subject to the *Privacy Act 1988* (Cth).

The *Australian Bureau of Statistics Act 1975* establishes the ABS as an independent statutory authority. Section 6 prescribes its functions to include the collection, compilation, analysis and dissemination of statistics and related information.

The *Census and Statistics Act 1905*:

- empowers the Australian Statistician to collect statistical information on a broad range of demographic, economic, environmental and social topics;
- enables the Australian Statistician to direct a person to provide statistical information, in which case they are legally obliged to do so;
- requires the ABS to publish the results of these statistical collections;
- places a life-long obligation on all ABS officers to maintain the secrecy of information collected under the Act, and provides harsh penalties for those who fail to do so; and

- does not allow data to be published in a manner that is likely to enable the identification of a particular person or organisation.

The ABS undertakes the Census every five years in accordance with the *Census and Statistics Act 1905*. Names and addresses are among the matters in relation to which the Statistician may collect information, as prescribed by regulation 6 and Schedule 1 of the *Census and Statistics (Census) Regulations 2005* (Cth).

The proposal to permanently retain name and address information from responses to the 2016 Census does not involve the collection of additional information than that collected in the 2011 Census.

The *Census and Statistics Act 1905* requires the ABS to publish results in a manner not likely to identify a particular person, household or organisation. Section 19 of the *Census and Statistics Act 1905* forbids past or present officers of the ABS (which includes temporary staff) from divulging information collected under this Act, either directly or indirectly, under penalty of up to 120 penalty units (currently $21,600) or imprisonment for two years, or both. To ensure that confidentiality and privacy provisions are observed, all officers of the ABS sign legally binding undertakings to comply with the secrecy provisions of the *Census and Statistics Act 1905*. These undertakings are binding for life and are renewed annually.

The ABS also has an obligation to comply with the *Privacy Act 1988*, including the Australian Privacy Principles. The Australian Privacy Principles regulate how the ABS may collect, use, disclose and store personal information. In accordance with Australian Privacy Principle 3, the ABS may collect personal information (such as name and address) where it is reasonably necessary for, or directly related to, its functions or activities. Australian Privacy Principle 11 provides that the ABS may retain the personal information of an individual where that information continues to meet a business need that is aligned with the purpose for which the information was collected.

The proposal to retain names and addresses from responses to the 2016 Census is consistent with the functions of the ABS prescribed in the *Australian Bureau of Statistics Act 1975* and compliant with all the provisions in the *Census and Statistics Act 1905* and the *Privacy Act 1988*, including the Australian Privacy Principles.

2.3. Governance and Institutional Arrangements

The ABS is Australia's national statistical agency, providing trusted official statistics on a wide range of economic, social, population and environmental matters of importance to Australia. A recent independent survey showed that trust in the ABS remains high and that 81 per cent of the general public and 100 per cent of informed users trust Australia's official statistical organisation, the ABS.

The ABS and its staff uphold the Australian Public Service (APS) Values and Code of Conduct. These values, which are congruent to the ABS's role as an independent provider of statistical information for Australia, are summarised in the following table:

Impartial	The APS is apolitical and provides the Government with advice that is frank, honest, timely and based on the best available evidence.
Committed to Service	The APS is professional, objective, innovative and efficient, and works collaboratively to achieve the best results for the Australian community and the Government.
Accountable	The APS is open and accountable to the Australian community under the law and within the framework of Ministerial responsibility.
Respectful	The APS respects all people, including their rights and their heritage.
Ethical	The APS demonstrates leadership, is trustworthy, and acts with integrity, in all that it does.

The ABS has a long history of, and a strong culture for, protecting the privacy of individuals and the confidentiality of information supplied by them. The protection of privacy is considered paramount to the successful conduct of the Census. The ABS maintains a Privacy Policy which sets out its personal information handling practices. The ABS Privacy Policy can be found at www.abs.gov.au/privacy. The Census Privacy Statement will be released before August 2016 and will be found at www.abs.gov.au/census.

In 2012, the ABS became an accredited Integrating Authority under the Commonwealth statistical data integration interim arrangements. Statistical data integration involves combining data from different sources to provide enhanced datasets for statistical and research purposes – which excludes purposes such as delivery of services to particular individuals, individual compliance monitoring, client management, incident investigation, or regulatory purposes.

As an accredited Integrating Authority, the ABS has been authorised as a safe and effective environment for data integration projects involving Commonwealth data. The ABS was accredited against the following criteria:

- ability to ensure secure data management;
- information that is likely to enable identification of individuals or organisations is not disclosed to external users;
- availability of appropriate skills;
- appropriate technical capability;
- lack of conflict of interest;
- culture and values that ensure protection of confidential information and support the use of data as a strategic resource;
- transparency of operation; and
- existence of an appropriate governance and institutional framework.

A copy of the accreditation claims made by ABS, which have been verified by an independent auditor, is available through the National Statistical Service website.

Consistent with its accreditation status, the ABS has well-established governance infrastructure and procedures to manage the approval, conduct and review of statistical data integration projects undertaken by the ABS. A Senior Committee comprised of senior level ABS staff (SES Band 2 / SES Band 1 level) oversees this process. All data integration projects undertaken by the ABS must be approved by the Committee prior to integration commencing. Approval is based on a written application endorsed by the project owner (SES Band 1 level) which covers the proposed data and risk management strategies for the project. Projects which the Committee deem to be 'high risk' under the Commonwealth Data Integration Risk Assessment Guidelines require approval by the Australian Statistician. Project owners must notify the Committee of any proposed amendments to their project, and if a major amendment is needed, submit a new proposal for approval. In the interests of transparency, outlines of approved data integration projects within scope of the Commonwealth arrangements are published on the ABS website.

2.4. Retention and Use of Information

The Census collects information relating to each person and household in Australia. While the Census collects information relating to each person and household in the country, it is not concerned with information about individuals as such. The Census is taken to provide information about the community as a whole and about groups within the community. The public expects that the information they provide will be kept confidential.

Protection of personal privacy is paramount at the ABS. Based on a strong track record, people can be confident that the ABS will keep their personal information secure – both that provided on paper Census forms and the online eCensus.

The ABS proposes to retain names and addresses from responses to the 2016 Census for statistical and operational purposes within the existing protective legislative and procedural frameworks, with no disclosure of identifiable personal information.

Consistent with Australian Privacy Principle 11, name and address information would only be retained where there continues to be a business need for doing so. After processing of the Census data, names and addresses would be separated from other personal and household information on the Census data set. Names and addresses would also be separated from each other. Names would not be brought back together with other information collected from respondents to the Census. Anonymised versions of names would be generated for data integration purposes and addresses geocoded.

This Privacy Impact Assessment will inform the decision on whether the ABS will retain the names and addresses collected from responses to the Census; the outcome of this decision will be published by the end of 2015. If a decision is made to proceed with the proposal, the ABS will ensure transparency of this decision and how personal information will be managed, consistent with Australian Privacy Principle 1. It will do this by:

1. publishing the decision and the privacy impact assessment on the ABS website by the end of the year;
2. detailing how Census name and address information would be held and used by the ABS in the publication – 'How Australia takes a Census', to be published in March 2016;
3. releasing the Census Privacy Statement before the 2016 Census; and

4. publishing responses to frequently asked questions for participants of the Census.

2.5. Information Flows

Following the completion of Census processing, the ABS proposes to permanently separate name and address information from other information on the Census dataset, and to store names and addresses separately from other data and from each other, and securely. This separation is considered a key element of the privacy design, protecting against the accidental or malicious disclosure of personal information from responses to the 2016 Census.

The separation principle would be enforced to separate name and address variables from analysis or content information during both data storage and use in statistical data integration or for operational purposes. The separation principle is a well-established approach applied internationally to protect privacy and the security of data by ensuring that no-one working with the data can view both identifying information (such as name and address) together with the analysis or content data (such as country of birth or educational attainment).

As an accredited Integrating Authority, the ABS has been audited and accredited for its application of the separation principle for the purposes of statistical data integration activities.

Under the separation principle, authorised ABS officers would only have access to the information required to support their role. That is, separation would be functionally based. This means that only a limited number of ABS staff would have access to the retained information.

The key layers of protection that would be in place as a result of applying functional separation are:

- names, anonymised names and addresses would be stored securely and separately to each other and to other Census data;
- access to name, anonymised name and addresses is restricted and approved on a need-to-know basis;
- names would be used to generate anonymised versions of names to use as linkage keys in statistical and research projects that have been assessed and approved consistent with the *Commonwealth Statistical Data Integration principles, governance and institutional arrangements*; and
- neither names nor anonymised names would be part of a Census analytical file, nor would they ever be disclosed by the ABS.

The proposed functional separation roles as applied for data integration projects are outlined in Box 1.

Box 1. Functional Separation Roles

Functional separation involves placing project members into separate roles during the lifecycle of a data integration project. Access to data will vary depending on the role that each project member performs. Under the separation principle, any one staff member is prevented from accessing both identifying and analytical information from datasets during the linkage process.

There are four roles, as follows, of which the first two are most relevant to the proposal:

Librarian: A staff member in this role performs processes such as the acquisition of data to be used for linking purposes, standardisation of the data and creation of the files for input into linking. Separation is maintained by staff only performing one role at a time per project. Librarians may also be responsible for creating anonymised linkage keys for names for additional or new datasets such as survey and administrative data. These anonymised keys would be stored separately to the file containing names.

Linker: A staff member in this role performs the linkage of the two datasets. Their access is limited to fields they require for linking and clerical review (when applicable), which can include identifying information such as anonymised name and address.

Assembler: A staff member in this role takes the linked outputs (from the linker) and combines them with the analysis variables provided by the data custodian. At this point a new identifier, 'Analysis identifier', is created for research and analysis to be undertaken.

Analyst: A researcher in this role performs analysis on the linked dataset. Their access is limited to data needed for analytical purposes, which typically does not include identifying information.

Staff in the above roles are provided with access to data on a need-to-know basis by a designated Role Manager, with access restricted to either the linking or the analysis information based on their data requirements.

The process flows for the retention of names and addresses from responses to the 2016 Census are outlined below.

Name Information

Once Census processing is complete, names would be separated from the remainder of the Census dataset, and retained in a separate file as long as there is a purpose for doing so (consistent with Australian Privacy Principle 11). Names would not be brought back together with other information collected from respondents to the Census. Anonymised versions of names would be generated from the names and stored separately from both the file of names and the Census dataset. The name and anonymised name files would be the responsibility of functionally separate sections in the ABS.

Access to and use of the name file would be restricted and subject to approval from a senior officer in order to create new anonymised versions of names to ensure linkage keys for statistical data integration keep pace with evolving standards and methodology and are fit-for-purpose.

The anonymised name file would be used as a resource for data linkage research and practice, forming part of the foundational infrastructure underpinning ABS statistical data integration activities involving Census data.

Neither names nor anonymised names would be part of a Census analytical file, nor would this information ever be disclosed by the ABS.

The functional separation approach is consistent with international best practice, and is utilised effectively by the Office of National Statistics in the United Kingdom, Statistics New Zealand and Statistics Canada, for example.

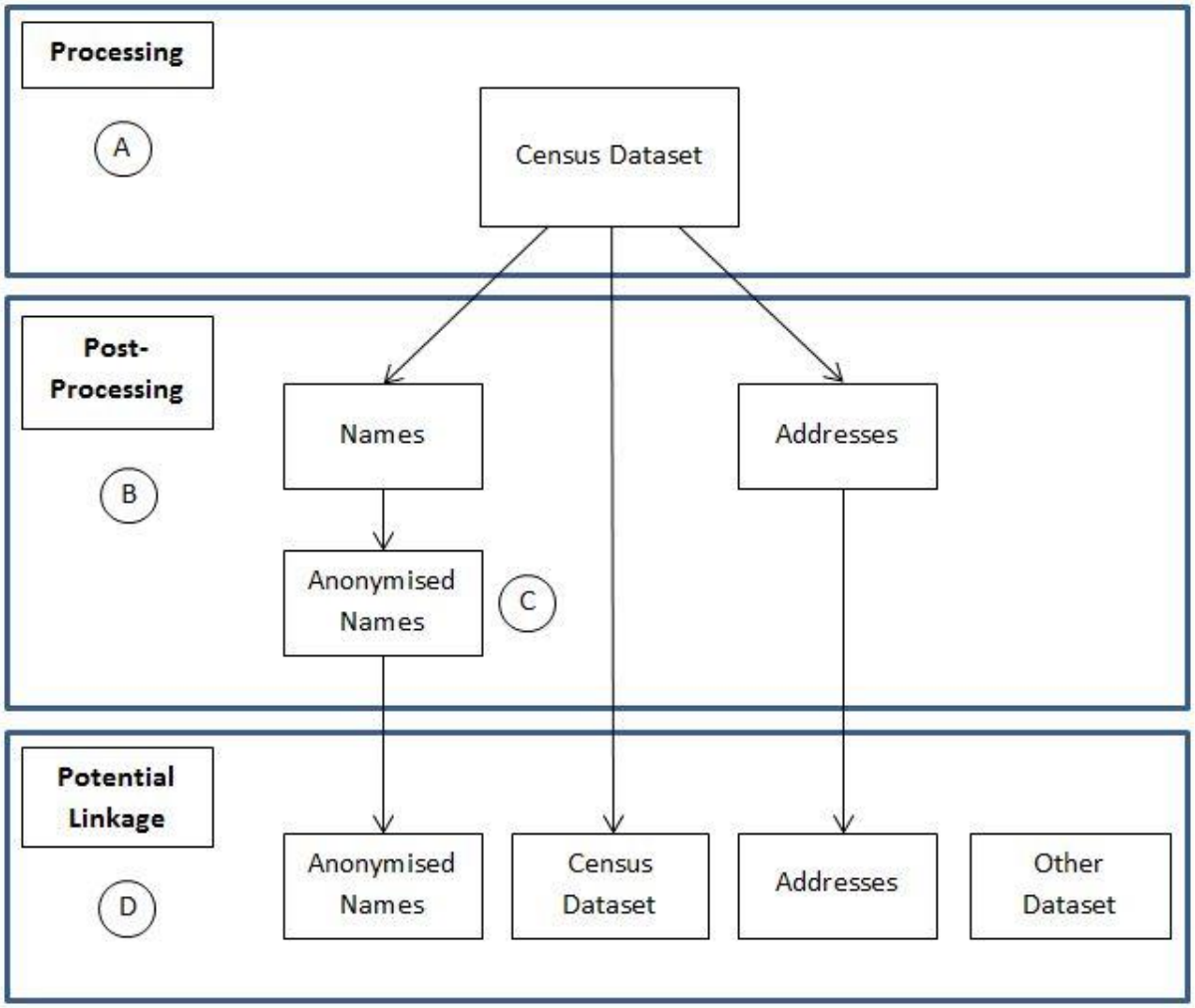
Address Information

Once processing is complete, addresses and their associated coordinate geocodes would be retained separate to the Census dataset as long as there is a purpose for doing so (consistent with Australian Privacy Principle 11). This file would only be for internal use.

Once separated from the Census dataset, addresses would not be brought back together with other personal and household information in the Census dataset. A senior staff member (e.g. Executive Level 2) would have responsibility for the address file.

Address information from the 2016 Census would be used to support the improvement of geospatial statistics, the ABS Address Register, and other operational efficiencies.

Figure 1. Map of Information Flows



A. ABS 2016 Census staff will collect and process data from the 2016 Census.
B. Once processing is complete, names and addresses would be permanently separated from the remainder of the Census dataset, and stored securely in separate files with restricted access.
C. Anonymised versions of names would be generated from the names; these would be stored separately from both the file of names and the Census dataset. ABS staff in the librarian role would perform these functions.
D. For approved data integration projects involving 2016 Census data, staff in the librarian role would recombine demographic and anonymised name information on an as-needed basis to allow the Census dataset to be used for statistical data linkage. ABS staff in the linker role would perform the linking.

2.6. Security of Information

The ABS has an embedded culture of security and compliance, and has established robust and effective processes to protect the integrity and privacy of information collected from individuals and businesses.

The ABS complies with the mandatory requirements established by the Australian Commonwealth *Protective Security Policy Framework*. The Protective Security Policy Framework provides the appropriate controls for the Australian Government to protect its people, information and assets, at home and overseas.

The ABS also takes reasonable steps to comply with the Office of the Australian Information Commissioner's *Guide to information security* and *Guide to handling personal information security breaches*.

Governance Security

To enhance physical, IT and systems security, the ABS has established governance arrangements including reporting to the portfolio Minister (the Treasurer) on compliance with the Protective Security Policy Framework, implementing risk management policies and strategies, and creating and maintaining security plans.

The ABS has a rolling annual audit program, including audits of protective security (which focusses on different areas such as building access, document handling and contractors), information security and access (which focusses on different systems such as secure deposit box, email, computer assisted interviewing, and laptops). These audits are undertaken annually.

Personnel and Physical Security

All ABS staff and contractors who require unescorted access to ABS premises are required to undergo a pre-employment suitability and eligibility assessment. This requirement may be waived in certain circumstances, such as confirmation from the vetting authority that the person has recently obtained a National Security clearance. New employees also undergo police checks and are required to make a declaration of interests to ensure there are no conflicts of interest prior to employment commencing.

Access to ABS physical premises, excluding public areas, is at all times restricted to approved persons, and controls such as an electronic access control system, sign-in registers, reception personnel and security guards are in place.

Information Security

The ABS recognises and strongly respects the information security responsibility it bears as a result of retaining names and addresses. People can be confident in the numerous and robust security measures implemented by the ABS to safeguard their data to prevent identity theft or misuse of data.

The ABS has an excellent track record of data security, with few serious breaches over its history, and is committed to ensuring this position continues into the future. The prosecution and conviction

of a former staff member for an economic data breach (not a privacy breach) demonstrates that the ABS and the Australian judicial system has no tolerance for malicious acts of data breach and the ABS will not hesitate to apply the full authority of the law to these acts. Such a breach was unprecedented in ABS' 110 year history and resulted in an independent review of security arrangements (the Gibson Review). The outcome of the review was a set of recommendations, all of which were implemented, resulting in greater assurance that sensitive information in the possession of the ABS is more secure and controls on information stores are more robust. The ABS also applies secure practices to avoid accidental breaches.

The ABS information technology environment has comprehensive security measures in place, including Australian Signals Directorate Strategies to Mitigate Targeted Cyber Intrusions[6] and industry best practice.

In 2014, the ABS was one of seven government agencies which handle sensitive information whose information security strategies and related controls were assessed by an Australian National Audit Office cross-agency audit.[7] The audit examined ABS' overall security position. The ABS was ranked as the most compliant with the 'Top Four' mandatory mitigation strategies against cyber intrusions. The ABS was also rated as an Internally Secure Zone i.e. as having security controls in place which provide protection against breaches and disclosures of information from internal sources.

A key protection against identity theft is the 'privacy by design' concept to address personal information security. The ABS is compliant with the Australian Government's core security policies (the Protective Security Policy Framework and Information Security Manual) and have designed privacy into the application of whole of government information security. Email servers and gateway security have been configured to block emails containing the marking 'Sensitive: Statistics', and this in turn reduces the likelihood of accidental data leakage via digital means.

The current information security practices that are in place within the ABS to safeguard data include:

1. high level encryption of data, including tight security around the storage and creation of the encryption keys;
2. an audited linking environment, involving staff activity being logged, monitored and, if inappropriate activity is found, investigated. Any misuse would result in immediate termination of access for the staff member, with further sanctions imposed if necessary;
3. ABS staff and in-posted officers sign legally binding Undertakings of Fidelity and Secrecy to ensure they are aware of their obligation to protect confidential information, and the consequences of disclosure (which include criminal penalties);
4. enforcement of the clear desks and clear screen policy;
5. access on a 'need to know' basis;
6. annual IT audits;
7. Vulnerability Assessments are carried out on all new IT Systems by specialised staff in IT Security trained in the field of Ethical Hacking;

[6] http://www.asd.gov.au/infosec/mitigationstrategies.htm

[7] Australian National Audit Office Audit Report No.50 2013–14, *Cyber Attacks: Securing Agencies' ICT Systems*, http://www.anao.gov.au/Publications/Audit-Reports/2013-2014/Cyber-Attacks-Securing-Agencies-ICT-Systems/Audit-summary.

8. ethical hacks carried out every 12 months on existing systems;
9. Protective Security Management Committee reviewing security risks quarterly;
10. ongoing reporting of compliance with Government Security Policy including the Protective Security Policy Framework and Australian Signals Directorate Information Security Manual.

In addition to the information security practices described above, the ABS would apply the separation principle (refer to Section 2.5 for detail) to ensure that name and address files are stored securely, access is granted on an approved need-to-know-basis, and that no one working with the data can view both identifying information (name and address) at the same time as analysis information (such as country of birth or educational attainment).

These combined measures would safeguard retained name and address information and address confidentiality, privacy, identify theft and security risks.

2.7. Disclosure of Information

In accordance with the *Census and Statistics Act 1905*, name and address information from the 2016 Census, as well as outputs from any secondary integrated datasets using Census data, would not be disclosed, published or disseminated in a manner which is likely to enable the identification of a particular person, household or organisation.

Section 19 of the *Census and Statistics Act 1905* makes it an offence for any past or present ABS officer to divulge, either directly or indirectly, any confidential information collected under this Act. The Act provides for heavy criminal penalties (fines of up to $21,600 or imprisonment for 2 years or both) for anybody convicted of breaching this obligation - even if they are no longer employed by the ABS. Staff are required to sign Undertakings of Fidelity and Secrecy which are renewed annually.

2.8. Access to and Correction of Information

In accordance with Australian Privacy Principles 12 and 13, respondents have the right to request access to their personal information held by the ABS and to request its correction. This is clearly stated in the ABS Privacy Policy, which is publically available on the ABS website. If such a request is made, the ABS would respond within 30 days. No charge is made to individuals for requesting access to or correction of their information, or for access being granted.

A decision by the ABS to grant a privacy request to access or correct an individual's personal information would take into account whether the ABS is required or authorised to refuse the request under relevant legislation including the *Freedom of Information Act 1982* or any other Commonwealth legislation which provides for access by persons to documents, in particular the *Census and Statistics Act 1905.*

The ABS Privacy Policy provides information and contact details for individuals who are concerned that the ABS may have breached its responsibilities or their privacy rights. The ABS acknowledges complaints within five business days of receipt, and will investigate and respond within 30 days for non-complex matters.

3. Stakeholder Consultation

The ABS sought public submissions on both the nature and content of the 2016 Census from November 2012 to May 2013. In August 2015, the ABS published and promoted the 'Census of Population & Housing: Nature and Content, Australia, 2016' which highlighted that the ABS is considering the retention of both names and addresses for statistical purposes. In October 2015, the ABS published the 'Information Paper: Census of Population and Housing – Proposed Products and Services, 2016' which highlighted that data integration will continue to be a central element of the Census.

In order to understand contemporary community expectations, the ABS conducted a series of 16 focus groups across the country (in both metropolitan and regional locations), arranged through a market research company, in order to understand public attitudes and acceptability of the retention of name and address information from the Census. The focus group testing found that the ABS was seen as a trustworthy organisation producing important data for decision making, with the vast majority of participants having confidence that the personal data they provide to the ABS is kept safe and secure. This finding was consistent with the results from a recent independent survey which found that trust in the ABS remains high and that 81 per cent of the general public and 100 per cent of informed users trust Australia's official statistical organisation, the ABS.

More specifically, feedback from focus group testing indicated a general level of support for retaining names and addresses, and the use of anonymised linkage keys for the purposes of ensuring a higher accuracy in the linkage rate than is currently possible for joined up datasets. In particular, there was a general view that it was important that this work was of sufficient quality to enable accurate monitoring of trends over time. Participants also held concerns about the quality and usefulness of current linked datasets that had lower linkage rates of around 60% - 70%. In working through examples, focus groups were generally comfortable with the protections that the ABS would put in place to preserve privacy and confidentiality on the proviso that the ABS be transparent about how it handles people's personal information.

Following the above preliminary stakeholder consultation processes, the ABS directly notified key internal and external stakeholders of its proposal to retain names and addresses from responses to the 2016 Census in November 2015, and invited feedback to inform this Privacy Impact Assessment and the final decision on whether to adopt the proposal

The ABS publicised its intent to conduct a Privacy Impact Assessment by publishing a Statement of Intent on the ABS website in November 2015, as well as a Media Release directing attention to the Statement of Intent. Both releases included an invitation to comment and provided contact details to facilitate this.

The Office of the Australian Privacy Commissioner was consulted throughout this Assessment and will continue to be consulted in the lead up, and during, the conduct of the 2016 Census. Contact with the State and Territory Privacy Commissioners or relevant representatives for each State and Territory on this matter was made via a letter and copy of the Statement of Intent and Media Release. No substantive privacy-related concerns were raised by these offices.

Media coverage consisted of two articles of which the nature was informative and favourable. Articles appeared in IT News (12/11/2015) and PS News (13/11/2015).

Public feedback consisted of three responses from private citizens who all raised concerns with the proposal.

After consideration of this Privacy Impact Assessment and of all feedback received, the ABS will decide whether to proceed with the proposal to retain names and addresses from responses to the 2016 Census. The outcome of this decision will be published in December 2015, and will be further described in the March 2016 publication of 'How Australia takes a Census' and reflected in the Census Privacy Statement.

4. Privacy Risk and Mitigation

4.1. RISK: Unauthorised access by ABS staff to data stored in the ABS environment

Likelihood: Very low.

Consequence of breach: ABS staff may inadvertently or maliciously identify an individual.

Management of risk: To guard against identification of an individual, and any subsequent misuse of their personal information, by an ABS staff member, the functional separation principle and security arrangements will be implemented, as detailed in Sections 2.5 and 2.6.

Management of data breach: Depending on the circumstances, the ABS will:

- Take reasonable steps to comply with the guidelines for handling personal information security breaches established by the Office of the Australian Information Commissioner;
- Notify affected individuals of the breach;
- Implement immediate mitigating controls to prevent further spreading of the breach;
- Involve ABS security, senior line management and where necessary, the police.

4.2. RISK: Unauthorised non-ABS access to data stored in the ABS environment

Likelihood: Very low.

Consequence of breach: The consequences of breach of privacy depend on whether names, anonymised names, or linked data is accessed.

- If names or addresses are accessed, individuals or households are likely to be directly identifiable but no other information about the individual would be available
- Data contained in anonymised or linked datasets will only be brought together by anonymised linkage keys and is unlikely to enable direct identification of an individual or household.

Management of risk:

- Functional separation principle implemented – see Sections 2.5 and 2.6 for details;
- names, anonymised names and addresses would be stored securely and separately to each other and to other Census data;
- access to names, anonymised names and addresses is restricted and approved on a need-to-know basis;
- neither names nor anonymised names would be part of a Census analytical file, nor would they ever be disclosed by the ABS.
- All ABS data, including names and addresses, are stored in a secure environment in accordance with the mandatory requirements of the Australian Government Protective Security Policy Framework (PSPF) and consistent with the Information and Communications Technology Security Manual (ISM).

Management of data breach: Depending on the circumstances, the ABS will:

- Take reasonable steps to comply with the guidelines for handling personal information security breaches established by the Office of the Australian Information Commissioner;
- Endeavour to recover the data;
- Implement immediate mitigating controls to prevent further spreading of the breach;
- Notify affected individuals of the breach;
- Involve ABS Security and the Australian Federal Police.

4.3. RISK: Accidental release of name and/or address data in ABS outputs or through loss of work related IT equipment and IT documentation

Likelihood: Very low.

Consequence of breach: Name and/or address information is publically released.

Management of risk:

The ABS already successfully manages and protects the privacy of Australians throughout data integration processes involving sensitive datasets, including the Census, and thus effective privacy protections are already in place and in practice.

ABS staff are legally obliged to ensure that data will not be released in a manner which is likely to enable the identification of a person. This is a requirement under the *Census and Statistics Act 1905*; under the Act, ABS staff are subject to criminal penalties if found guilty of breaching its secrecy provisions. Annually, ABS staff sign legally-enforceable undertakings acknowledging that they understand their legal obligations as well as undertake training on the handling of personal information.

The separation principle will be enforced to separate names and addresses from analysis or content information during data storage, linking and analysis. Names and addresses will never be re-joined back with Census data.

Staff who require access to name and address information from the Census for their approved role will only access this information through secure electronic server environments, reducing the risk of an accidental release of personal information through potential loss of IT equipment such as a laptop or work documents (for example: emails).

Management of data breach: Depending on the circumstances, the ABS will:

- Take reasonable steps to comply with the guidelines for handling personal information security breaches established by the Office of the Australian Information Commissioner;
- Endeavour to recover the data;
- Notify affected individuals of the breach;
- Involve ABS security, senior line management and where necessary, the police.

4.4. RISK: Reduction in participation levels in ABS collections due to loss of public trust

Likelihood: Very low

Consequence: The proposal to retain names and addresses from responses to the Census may cause public concern which results in a reduction of participation levels in ABS collections, and/or a public backlash.

Management of risk: To mitigate this risk, the ABS:

- Has informed Commonwealth, State and Territory Information and Privacy Commissioners of the proposal and has committed to addressing any feedback;
- Sought feedback from the public through publication of a Media Release and a Statement of Intent to conduct a Privacy Impact Assessment;
- Will comply with established legislative and procedural frameworks which safeguard privacy and data security;
- Will be transparent about objectives, processes and outcomes;
- Will prepare responses to frequently asked questions and ensure Census Field Officers are equipped to respond to concerns from respondents.

Management if risk eventuates: Depending on the circumstances, the ABS will:

- Respond to concern from the media, stakeholders and the public;
- Conduct further consultations;
- Reconsider the privacy design for the proposal, if required.

4.5. RISK: 'Function creep' – unintentional expanded future use of retained name and address information

Likelihood: Very low

Consequence: In the future, name and address information from responses to the 2016 Census may be used for purposes beyond what is currently contemplated by the ABS.

Management of risk: Compliance with the legislative and governance framework described in Sections 2.2 and 2.3 will guard against function creep by ensuring that:

- names and addresses are retained in accordance with the Australian Privacy Principles;
- any data integration project involving retained information is undertaken for statistical and research purposes only;
- no information will be released in a manner which would enable the identification of a person or household.

In addition, usage of name and address information from responses to the 2016 Census will be subject to established approval, evaluation and review procedures including:

- Internal approval processes, as described in Section 2.3, for data integration projects which assesses the benefits and risks of each project and their compliance with ABS policies;
- Periodic reviews of policies including the policy on retention of personal information and the privacy policy, to ensure these policies are achieving their objectives, are implemented in practice, and remain aligned with public commitments made by the ABS;
- Annual internal audits of information and protective (physical) security.

Management if risk eventuates: Depending on the circumstances, the ABS will:

- Consult affected stakeholders;
- Review relevant internal policies.

5. Conclusion

The outcome of this Privacy Impact Assessment has determined that the proposal to retain names and addresses from responses to the 2016 Census is consistent with the functions of the ABS prescribed in the *Australian Bureau of Statistics Act 1975* and compliant with all the provisions in the *Census and Statistics Act 1905* and the *Privacy Act 1988*, including the Australian Privacy Principles.

In relation to the proposed retention of names and addresses from responses to the 2016 Census, a small number of potential risks to personal privacy and public perception have been identified. This Assessment concludes that in each case, the likelihood of the risks eventuating is 'very low'. It also concludes that the ABS has implemented robust processes to manage data and protect privacy, and that these arrangements effectively mitigate these risks. Any residual risks are such that the ABS is capable of managing.

Recommendations

In accordance with the above conclusions, it is recommended that the ABS:

1. Retain names and addresses from responses to the 2016 Census.
2. Update the Census Privacy Policy prior to conducting the Census on 9 August 2016 to ensure the Australian public are informed that names and addresses from responses to the 2016 Census will be retained by the ABS for statistical and operational purposes as long as there is a purpose for doing so.
3. Implement business processes which are necessary to manage the separation and retention of names and addresses from responses to the 2016 Census.
4. Develop training and support materials for staff accessing name and address data as well as guidelines for ABS Census Field Officers, and publish online responses to frequently asked questions concerning the retention of names and addresses from responses to the 2016 Census to support queries from the public.
5. Conduct an internal audit of the implementation of the above recommendations as part of the internal audit program scheduled for the 2017-2018 financial year.
6. Assign responsibility to a senior committee for monitoring whether there is an ongoing need for the retention of name and address information.

Appendix A – Media Release

MEDIA RELEASE

11 November 2015 Embargo: 11:30am (Canberra Time)

ABS to conduct a Privacy Impact Assessment

The Australian Bureau of Statistics (ABS) today announced it will conduct a Privacy Impact Assessment on the retention of names and addresses from responses to the 2016 Census of Population and Housing.

The ABS is considering the retention of names and addresses as a key enabler for improved household surveys and high quality statistics.

The retention of names and addresses would support the integration of Census data with other survey and administrative data to provide a richer and dynamic statistical picture of Australia.

Historically, the ABS has destroyed all name and address information after statistical processing of the Census has been completed.

In considering this change, the ABS remains committed to maintaining high levels of community trust. No information will be released in a way that would enable users of Census data to identify any particular individual or household. Names and addresses will be separated from other household and personal data collected in the Census. Addresses and anonymous versions of names will only be used for approved projects.

To inform both our decision and approach, the ABS will undertake a Privacy Impact Assessment (PIA) and is seeking feedback on this proposal.

Further information is contained in the ABS Statement of Intent. To provide feedback on the proposal, please write to privacy@abs.gov.au by 2 December 2015.

Appendix B – Statement of Intent

Statement of Intent
ABS to conduct a Privacy Impact Assessment on retention of names and addresses from responses to the 2016 Census

The ABS has a long and proud history of Census taking in Australia, and the 2016 Census will be the seventeenth national Census of Population and Housing. The Census is the largest collection the ABS conducts, and one of the most important. The protection of the privacy and confidentiality of every person and household in Australia is of the highest priority. Maintaining the trust that the community has in the ABS is also paramount.[8]

The 2016 Census will introduce significant changes to the way the Census is conducted, with a move to a digital-first approach. Australia's first predominantly digital Census will be faster, more efficient and easier for the public.

The 2016 Census will also provide an opportunity to improve and expand the information available to Australians through continuing the use of statistical data integration techniques to bring together 2016 Census data with previous Censuses (2006 and 2011) and other high value research datasets. Together these initiatives will continue to provide new insights and ensure the Census delivers maximum benefit to governments and the community. For information on current Census data integration initiatives please follow the link.

Building on the successes of the 2006 and 2011 Censuses, the ABS intends to explore the retention of names and addresses from the 2016 Census to provide a benefit to the ABS and wider community by:

- enabling higher quality and more efficient linkage of high value survey and administrative datasets with the Census, particularly for small or highly mobile population sub groups of policy interest;
- supporting a range of organisational efficiencies, such as the development of an address register, improving sampling, imputation and provider management; and
- supporting more flexible geospatial outputs.

To give full effect to these changes, the ABS would need to cease the historical practice of the destruction of name and address information collected in the Census. The ABS proposes to instead apply well established separation principles to protect privacy by storing both name and address separately and securely from other household and personal data collected in the Census. This is an internationally recognised approach to protecting privacy and ensuring personal information is kept secure. Under this proposed approach, names will never be brought together with other Census data. Only anonymised versions of name will be used for approved statistical data integration

[8] Trust in the ABS remains high, with a recent independent survey showing that 81 per cent of the general public and 100 per cent of informed users trust Australia's official statistical organisation.

projects. Addresses will only be used for approved data integration, operational and geospatial purposes.

The ABS intends to conduct a Privacy Impact Assessment on the retention of names and addresses from responses to the 2016 Census. The Privacy Impact Assessment will ensure the right privacy design can be put in place and inform the processes, risks and risk mitigation strategies that would be required to enable the secure retention of name and address information from the 2016 Census.

At the completion of the Privacy Impact Assessment process, and after considering all feedback received, a decision will be made on whether to progress with the retention of name and address from 2016 Census responses. The outcome of this decision will be published on the ABS website by the end of 2015.

As our track record demonstrates, the ABS takes its role in protecting the privacy and confidentiality of all respondents very seriously. The Census and Statistics Act 1905 commits the ABS to protect the confidentiality of persons, households and organisations. The Privacy Act 1988 commits the ABS to protect privacy. The ABS recognises that protecting the privacy of individuals and the confidentiality of information supplied by them are paramount to the successful conduct of a Census. For more information on how we approach privacy and confidentiality in the Census please follow the link.

The ABS invites feedback on the retention of name and address from the 2016 Census. Any feedback should be provided in writing by close of business **Wednesday, 2 December 2015** to the following address: privacy@abs.gov.au**.**