Australian Bureau of Statistics

PRIVACY IMPACT ASSESSMENT

TableBuilder

September 2022

Contents

EXECUTIVE SUMMARY

TableBuilder is a secure analytics environment that provides safe access for users to produce aggregated table data from unidentified microdata. Registered users build their own tables which are automatically confidentialised.

Microdata is the unit record data that provides detailed information about people, households, businesses or other types of records. The microdata accessed by TableBuilder is "unidentified" data, as it has had all names, addresses and other direct identifiers removed as well as some other changes to the data to reduce the risk of re-identification. Further controls are applied in TableBuilder (through the Five Safes Framework), which means that data returned to users is aggregated.

As TableBuilder infrastructure pre-dates the OAIC's guidelines, a PIA has not previously been undertaken for the TableBuilder infrastructure. This PIA has been undertaken as a part of the ABS's commitment to good privacy practice and ongoing review and improvement of TableBuilder infrastructure.

This PIA has assessed the current state of TableBuilder infrastructure, including user registration and subsequent storage of personal information, as well as the TableBuilder infrastructure which enables users to build their own aggregate tables.

This PIA explores:

- data use and information flows - how the ABS collects, holds, manages, and discloses microdata and information about users of TableBuilder (section 2)
- compliance with the Australian Privacy Principles (APPs) (section 3)
- ABS response and next steps (section 4)

Analysis against the APPs found TableBuilder infrastructure and user registration to be compliant. Five best practice recommendations are presented to further enhance TableBuilder's privacy practices.

A summary this analysis and recommendations is provided at Table 1.

Table 1: Summary of recommended actions

APP	Compliance	Commentary	Best practice recommendations
APP1 – open and transparent management of personal Information	Compliant, but further action recommended	The ABS is committed to open and transparent management of the microdata that is accessed by TableBuilder. Relevant information is provided on the ABS Privacy Pages on the ABS website. ABS plans to update information on the website about the storage and security of microdata in TableBuilder.	*Recommendation 1: Update online materials and communications to provide information about the storage and security of microdata accessed by TableBuilder.*
APP5 – notification of the collection of personal information	Compliant, but further action recommended	To ensure Transparency, it is recommended that the Conditions of Use are reviewed and if required updated to ensure users understand how their personal information will be used and compliance with APP5.	*Recommendation 2: Review and if needed update Condition of Use to ensure users understand how their personal information will be used and compliance with APP5.*
APP 11 – security of personal information	Compliant, but further action recommended	The ABS regularly reviews and takes reasonable steps to ensure the security of personal information of TableBuilder users.	*Recommendation 3: Implement any outcomes from security assessments to assure the continued security of personal information of TableBuilder users.* *Recommendation 4: Implement any outcomes arising from security assessments to assure the continued security of microdata in TableBuilder.* *Recommendation 5: Conduct a new PIA on the proposed TableBuilder move to cloud based services.*

PART 1. INTRODUCTION

1.1 Background

The Australian Bureau of Statistics (ABS) currently allows registered users to produce aggregated table data from unidentified microdata through ABS TableBuilder infrastructure.

TableBuilder gives registered users a tailored way of requesting the generation of customised tables from microdata, without the user having direct access to the microdata. Through privacy and confidentiality safeguards, the customised tables are not likely to enable the identification of an individual and can be downloaded and used publicly.

TableBuilder is currently hosted in the ABS tenancy of a Canberra based secure data centre. The ABS is authorised under Section 12 of the Census and Statistics Act, to release ABS aggregate data under certain conditions and manages access through the 'Five Safes' Framework. This is an internationally recognised framework for making effective use of data whilst controlling risks using several levers – safe people, safe projects, safe settings, safe data and safe outputs (Appendix D).

The ABS takes the responsibility to maintain its privacy commitment to the Australian people seriously. To do this, the ABS regularly reviews and makes improvements to security controls in response to the rapidly evolving cyber environment. This PIA has been conducted as a part of an ongoing commitment to review and improve TableBuilder infrastructure.

This PIA has assessed the current state of TableBuilder Infrastructure, including user registration and subsequent storage of personal information, as well as the TableBuilder table population processes. This assessment confirms:

- The unidentified microdata accessed by TableBuilder infrastructure may include some personal information.
- Registered users only access aggregated unidentified data which does not contain personal information.
- Registered users create table outlines from available datasets.
- Table population activities are separated from the user. Once all appropriate data confidentiality and suppression activities are applied, tables are only then available to the registered user for download.

- The resulting aggregated data in tables do not contain personal information and minimise the risk of re-identification of information.

Additional future work is planned to move to newer technologies and systems to improve TableBuilder. This planned work includes moving to cloud based infrastructure where additional security benefits can be leveraged. It is recommended that a future updated PIA be developed in parallel to support this work program.

1.2 Purpose, scope, and approach

Purpose

The Office for Australian Information Commissioner's (OAIC) guidelines recommend a PIA is undertaken for any project which will change how personal information is handled or stored, or for any changes an agency proposes which will:

"substantively change an existing activity or function. This includes a substantive change to the system that delivers an existing function or activity."

As TableBuilder infrastructure pre-dates the OAIC's guidelines, a PIA has not previously been undertaken for the TableBuilder infrastructure. This PIA has been undertaken as a part of the ABS's commitment to good privacy practice and ongoing review and improvement of TableBuilder infrastructure.

The TableBuilder infrastructure enables registered users to build their own aggregate tables by selecting the data items of their choice for cross-tabulation. Tables are automatically treated to protect privacy and confidentiality before the table (output) is provided. Users can use TableBuilder to perform a range of analysis, for more information see the TableBuilder User Guide.

This PIA reviews both the user registration process for use of TableBuilder, including the storage of user information and the TableBuilder infrastructure which enables users to build their own aggregate tables.

The purpose of this PIA is to:

- Consider the potential privacy impacts on people whose personal information has been provided to the ABS for statistical purposes and whose unidentified information underpins the tables requested by registered users through TableBuilder.

- Consider the privacy implications of the user registration processes and subsequent storage of user information.
- Identify privacy risks in relation to the Australian Privacy Principles (APPs) and community expectations.
- Identify, assess, and outline risk mitigation strategies to manage privacy impacts.

Scope

The ABS has developed standard operating and registration processes for TableBuilder, including data flows and the protections for managing personal information. This PIA assesses the APP compliance of:

- the use, disclosure, and storage of user information as obtained during the user registration process
- disclosure of tables to registered users
- the overall compliance of the TableBuilder infrastructure with the APPs.

Out of scope for this PIA is the assessment of APP compliance of the collection of statistical data by the ABS which is used by the TableBuilder infrastructure to produce tables.

Approach

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

- Mapping information flows
- PIA analysis and compliance check
- Addressing risks
- Development of this report
- Publishing the PIA or a PIA summary on the ABS website.

1.3 Personal and sensitive information

Personal information

Definitions

The Privacy Act defines "personal information" as:

> Information or an opinion about an identified individual, or an individual who is reasonably identifiable.

There are two overarching types of data involved in this project: microdata accessed by TableBuilder and data about users of TableBuilder.

System use of Microdata

Microdata is the unit record data that provides detailed information about people, households, businesses or other types of records. It includes data collected through ABS surveys and the Census, and person and business centred administrative data, and integrated data.

The microdata accessed by TableBuilder is unidentified, that is, it does not contain any personal identifiers. It has also had a number of confidentiality treatments applied to reduce the risk of re-identification of the information when tables are generated from TableBuilder. All microdata underpinning TableBuilder is carefully prepared, including:

- removal of all direct identifiers
- application of confidentiality methods applied to the data, such as top-coding and grouping.

These treatments are customised and tailored to address privacy risks specific to each dataset. Treatments used are described in more detail in the ABS Data Confidentiality Guide.

Microdata accessed by TableBuilder has overarching confidentiality governance managed by undertaking reviews of new and existing processes with:

- IT security and independent (IRAP) security assessments
- Methodology experts
- Disclosure Review Committee.

The ABS has a legislative requirement for the Australian Statistician to not release information 'in a manner that is likely to enable the identification of that person'. To reduce the risk of re-identification from tables the generated in TableBuilder, the system has further restrictions in place, including:

- not allowing users to view or access the microdata
- perturbing output in tables
- preventing cross-tabulation of certain variables.

The ABS uses the Five Safes Framework to minimise disclosure risk. The five safes work together to ensure the underlying microdata is protected and that the tables

produced by TableBuilder do not identify any individual. The application of the Five Safes framework to TableBuilder can be found in Appendix D.

The above combination of confidentiality control mechanisms and governance arrangements work together to ensure that personal information collected by the ABS for statistical purposes is not released through TableBuilder in a manner that is likely to identify individuals.

Information about users

The *Privacy Act 1988 (Cth)*[1] defines personal information as *"…information or an opinion about an identified individual, or an individual who is reasonably identifiable…"*[2].

Users include individuals who are applying to access or have been granted access to TableBuilder as well as ABS staff in auditor, administrator, or systems administrator roles. TableBuilder access processes collect, store and use information about users including some personal information such as:

- Name (first, surname)
- User's individual organisation email
- Phone number
- Physical street address when registering
- Organisation

This information is used by the ABS to appropriately administer user accounts. Some of this user information is shared with the registered users' organisations contact officer to manage accounts connected to their organisation.

1.5 Legislation and consultation

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

Consultation was conducted directly with WingArc Australia, the company responsible for the development of software used by TableBuilder. Targeted infrastructure consultation involved discovery and solution design recommendations.

[1] https://www.oaic.gov.au/privacy/the-privacy-act/
[2] https://www.oaic.gov.au/privacy/guidance-and-advice/what-is-personal-information/

ABS consultation with WingArc is ongoing due to the infrastructure dependency with TableBuilder.

1.6 Addressing community expectations

While the collection, use or disclosure of personal information may be authorised by legislation, this does not necessarily mean it meets community expectations.

The evidence from public sector research and community attitudes to data sharing and use (such as the Australian Data Strategy and OAIC's Australian Community Attitudes to Privacy Survey 2020) gives a good indication of expectations held by those whose privacy may be impacted by the project. These studies indicated the importance of transparency in how data is used and accessed and assurance that the data is kept secure with appropriate accountability mechanisms in place.

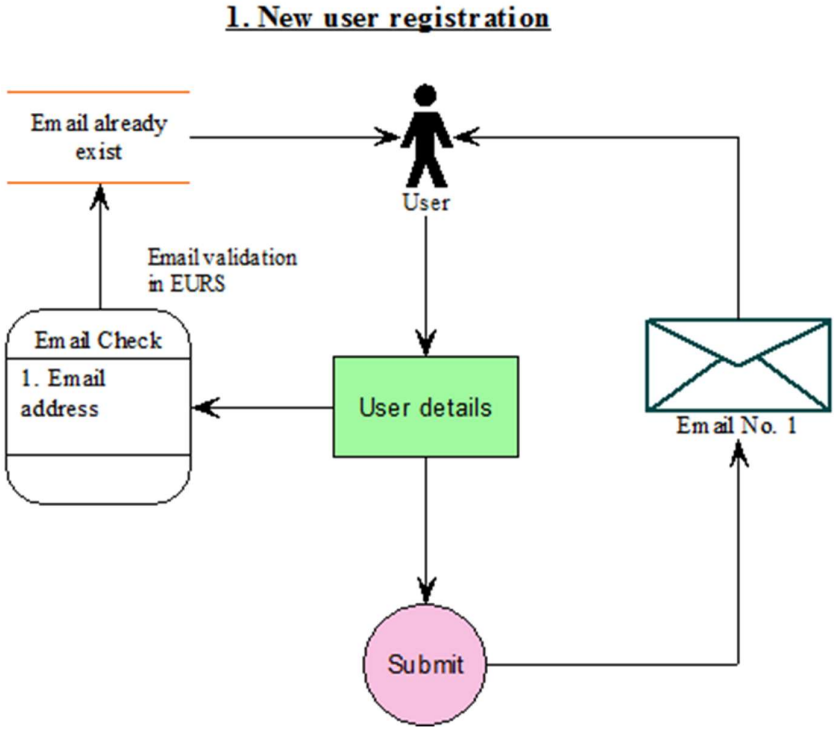
Public trust is critical to the ABS' reputation and to people's willingness to participate in ABS and government projects. While public consultation did not take place for this PIA, there was strong consideration of community attitudes and expectations regarding the project's privacy implications and risks. The ABS applies several security controls for the project to mitigate these concerns. These controls are detailed in Part 2 and 3.

PART 2. DATA USE AND INFORMATION FLOWS

2.1 User Registration

Personal information is collected from users as part of registering for a TableBuilder account. This information is required to verify the identity of users and helps to ensure the ABS is safely managing access to data. The user registration process is summarised in Figure 2 below.

Figure 2:



To register for TableBuilder access, the new user may be connected to a registered organisation. Registration of an organisation is facilitated through email.

User registration occurs through the ABS Registration Centre where they are asked to supply the following information:

- Email (registration with the email address of their organisation is recommended) *Mandatory*
- Password *Mandatory* 14 characters and contains at least 3 of the following:
  - upper case alpha
  - lower case alpha
  - number and
  - at least 1 special character
- Name (first and surname) *Mandatory*
  - Title *not mandatory*
- Telephone (work / home and or mobile) *Mandatory*
- Address (Street, suburb, country, postcode) *Mandatory*
- Secret question (including user defined answer) *Mandatory*

The ABS Registration Centre allows an external user to register themselves for access to ABS products.

Each registered user is given a unique user ID. The same user ID allows access to different products. Registered users can log into the ABS Registration Centre to update their personal details online at any time. Users request access to new products in TableBuilder via email.

There are three different types of registered TableBuilder users:

- TableBuilder user (researchers)
- Organisation Contact Officer
- ABS system administrators

The different TableBuilder functionality for these users is described in Appendix C.

There are additional controls and steps to add further protections to ABS system administrator users including:

- limiting the number of system administators
- only staff with a valid business need are provided access
- staff must undertake annual training on Privacy
- staff are subject to sanctions under the Public Service Act.

2.2 Table Creation

The user logs into TableBuilder using their assigned user ID and user created password. Once logged in, the user is presented with only the names of datasets they have been granted permission to generate tables from. The user selects the dataset they want to use. Tables are created based on an empty dataset containing only table metadata and then can be submitted to the table queue. TableBuilder populates all user requested tables through a job queue manager, which separates the data from the user. Once the table has been returned from the queue, the user can download the table of aggregate data as a file.

The job queue manager process further enhances security protections on the microdata by separating the user from the unit record data.

TableBuilder provides privacy and security protections on the underlying microdata through the system by:

- not allowing users to download individual records
- perturbing output in the aggregate tables
- preventing cross-tabulation of certain variables.

The combination of system architecture and data protections described in 1.3 – System use of microdata strengthens the security and privacy of the data. Privacy is considered at all stages and steps of TableBuilder operations. ABS activities to strengthen TableBuilder controls remain an on-going process.

2.3 Technology

The ABS User Registration Centre was built with EURS (External User Registration System) Web Services. All data is stored within the EURS Oracle database hosted on ABS private cloud infrastructure. The following information is stored in EURS: name, address, organisation, contact information, User ID, products available to users etc. The EURS system authenticates a user's UserID and passwords when logging into the ABS User Registration Centre or into the product application (eg TableBuilder).

TableBuilder frontend servers are hosted on ABS private cloud infrastructure in a network domain decoupled from the main ABS domain, these servers do not have any direct access to sensitive unit record data. TableBuilder database and backend job queue processing servers are hosted on ABS private cloud infrastructure. An AWS cloud hosted load balancer is used to direct incoming public traffic to the frontend TableBuilder servers. User account information is stored within the separate EURS system which TableBuilder utilises as its authentication provider.

2.4 Retention of information

The information that the ABS collects as part of the TableBuilder registration process is considered and treated as a Commonwealth Government Record and is stored, used and destroyed in accordance with the Archives Act 1983 and the Australian Privacy Principles, including keeping the data secure. Further information can be found within The National Archives of Australia.

PART 3. AUSTRALIAN PRIVACY PRINCIPLES

This PIA assesses privacy compliance of the project against the Australian Privacy Principles (APPs), which regulate the collection, use and disclosure of personal information by Commonwealth Agencies.

The following table summarises the main findings for the two aspects of this project, for TableBuilder user registration and for the TableBuilder infrastructure.

Australian Privacy Principle (APP)	Assessment	User Registration	Systems
APP1 – open and transparent management of personal information	Compliant	The ABS has a clear and up to date privacy policy which is publicly available. The collection of personal information from TableBuilder users is explicitly stated in the ABS Privacy Policy for Managing and Operating our Business. The policy outlines the types of personal information the ABS holds for users of ABS products like TableBuilder and how personal information is retained and then destroyed in line with current legislative requirements. Payment information for access to Census Pro and other TableBuilder datasets is retained and destroyed in line with the Public Governance, Performance and Accountability Act 2013.	The ABS is committed to open and transparent management of the microdata that is stored in TableBuilder. The ABS has a clear and up to date privacy policy on how the ABS handles personal information collected for the production of statistics which is publicly available – the ABS Privacy Policy for Statistical Information. The ABS plans to update information on the website about the storage and security of microdata in TableBuilder. *Recommendation 1: Update online materials and communications to provide information about the access to and security of microdata in TableBuilder.*
APP2 – Anonymity and Pseudonymity	Compliant	To facilitate access to TableBuilder and to ensure data is accessed appropriately ABS requires identification for organisations and individual users. The general rule (in APP 2.1) does not apply as it is impracticable for the ABS to deal with individuals who have not identified themselves or used a pseudonym.	n/a – collection of microdata used by the system is out of scope of this PIA.
APP3 – Collection of solicited personal information	Compliant	APP3 requires only the collection of information that is reasonably necessary. All data collected by ABS for managing TableBuilder access is reasonably necessary for the ABS to perform its	n/a – collection of microdata used by the system is out of scope of this PIA.

		function and safely manage access to, and use of, data in TableBuilder. All personal information is collected by lawful means. No sensitive personal information is collected. ABS also holds information of ABS employees that are administrative users, of the system. This includes basic personal information and is used as an added security measure to enable logging of any system actions and activities. Personal information about users is provided by the user directly into the ABS Registration Centre by the user. The use of personal information is stated in the Conditions of use at the time of registration	
APP4 – Dealing with unsolicited personal information	Compliant	ABS has appropriate measures in place to manage the receipt of unsolicited information. There are very few opportunities for a user to supply unsolicited personal information to the ABS. While it is possible for a user to include unsolicited personal information by email, it is handled in accordance with the ABS' usual policies for handling unsolicited information and destroyed and not stored as part of administering TableBuilder access arrangements. All ABS staff are required to complete annual privacy training which covers the handling of personal information.	n/a – microdata which underpins TableBuilder is generated from data already collected by the ABS for statistical purposes. As such, this PIA has not considered the impacts of APP4 on microdata for TableBuilder.
APP5 – Notification of the collection of personal information	Compliant, but further action recommended	The ABS understands the importance of transparency in informing individuals how their data is managed. Personal information is collected directly from users in the Registration Centre. The user is notified of how their personal information will be used through the Conditions of Use in the Registration Centre and via the ABS website. The user must complete the registration process to gain access to TableBuilder, and this includes setting up an account, supplying personal information and agreeing to the Conditions of use. These conditions state that the user agrees	A user's use of the system is recorded and may be used to audit the users use of the system for compliance against the conditions of use. The user is informed of this collection and use in the Conditions of Use in the Registration Centre and via the ABS website.

		"to provide true and correct information about my identity and contact details to the ABS in the Registration Centre, and if these details change, to provide the updated details to the ABS". To ensure Transparency, it is recommended that the Conditions of use are reviewed and if required updated to ensure users understand how their personal information will be used and compliance with APP5. *Recommendation 2: Review and if needed update Condition of use to ensure users understand how their personal information will be used and compliance with APP5.*	
APP6 – Use or disclosure of personal information	Compliant	ABS uses and discloses personal information collected in line with the uses and disclosures outlined in the APP6 collection notice. The use and disclosure of personal information for TableBuilder is outlined in the Conditions of use and noted in APP3.	TableBuilder will not change how the ABS collects personal information as part of the creation of microdata products. The user's use of the system is recorded and may be used to audit the users use of the system for compliance against the conditions of use. This use is in-line with the APP6 collection notice. The ABS may share with other organisations, confidentialised information about usage, for the purposes of usage reporting, auditing, feedback or performance. Any personal information collected will be held in accordance with the Privacy Act 1988. See ABS privacy policy and DataLab privacy notice for further information. This use is in-line with the APP6 collection notice.
APP7 – Direct Marketing	Not applicable	The ABS does not use or disclose personal information for direct marketing purposes. APP 7 is not relevant as it applies to organisations rather than to agencies like the ABS and the ABS has not been otherwise prescribed for the purposes of s 7A of the Privacy Act. We also note that direct marketing is not relevant to TableBuilder. Users may be contacted to let them know about new releases in TableBuilder.	

APP8 – Cross-border disclosure	Compliant	Both individuals and organisations located outside of Australia can be granted access to TableBuilder. As per APP6, the ABS may share personal information about an individual with the Contact Officer of an international organisation for the purpose of administering access to data and seeking approvals on an individual's behalf. This disclosure is stated in the Conditions of use which is accepted by the user during the registration process. The Contact Officer must also comply with conditions of use to ensure the overseas recipient does not breach the APP.	The ABS has taken reasonable steps to ensure that microdata accessed by TableBuilder is protected from misuse, unauthorised access or disclosure. TableBuilder infrastructure is located in Australia as set out in Part 2, Data and Information flows. TableBuilder provides privacy and security protections on the microdata by separating the user from the microdata. As with all users, no personal information is disclosed to users of TableBuilder. TableBuilder users only receive confidentialised aggregated data tables and have no direct access to the microdata.
APP9 – Government related identifiers	Not applicable	APP 9 does not generally apply to government agencies apart from some prescribed commercial activities. TableBuilder does not hold any Government related identifiers. AP9 is not applicable.	
APP10 – Quality of Personal Information	Compliant	APP10 requirements for TableBuilder are consistent with the assessment described in the MADIP and Cloud PIA updates, that ABS has adequate processes and systems in place that represent reasonable steps to ensure the quality of personal information. Information is provided on the ABS website to TableBuilder users about how to inform the ABS of changes to their personal information. Users can update their own information or when a request is received, ABS staff responsible for administering TabelBuilder can update personal information of users using the administrator user interface.	The collection of statistical information from individuals is out of scope of this PIA (APP10.1). Having regard to the purpose for which TableBuilder uses personal information (in the form of microdata) to produce aggregate statistics, no further steps are required to be undertaken to ensure the information is accurate, uptodate, complete and relevant (APP10.2).
APP11 - Security	Compliant, but further action recommended	All personal information collected by the ABS is protected in accordance with the Australian Government Protective Security Policy Framework and with the Australian Government records management regime. When no longer required, personal information is destroyed or deleted according to the National Archives of Australia's Administrative Functions Disposal Authority and our records authorities (2001/00000540 and 2007/00105946).	
		In addition, the ABS conducts regular security assessments. Key ICT platforms and	In addition, the ABS has taken reasonable steps to ensure that microdata stored in

		systems also undergo independent security assessments conducted by personnel accredited under the Australian Signals Directorate's Infosec Registered Assessors Program (IRAP). These thorough assessments ensure appropriate controls are in place to maintain the security of systems and data. *Recommendation 3: Implement any outcomes from security assessments to assure the continued security of personal information of TableBuilder users.*	TableBuilder is protected from misuse, unauthorised access or disclosure. The MADIP PIA Update outlines a range of protections of microdata covering legislative, protective security, information and communication technology and data governance controls. These findings are all relevant to the security of microdata accessed by TableBuilder. As set out in Part 2, Data and Information flows, TableBuilder provides additional privacy and security protections on the microdata through the system by: • not allowing users to download individual records • perturbing output in tables • preventing cross-tabulation of certain variables. Users can produce aggregated tables from TableBuilder by submitting their table to the queue for data retrieval, which separates the data and provides additional protection to the aggreged data. The ABS has a dedicated in-house IT security section and ABS Chief Security Officer dedicated to ensuring appropriate security risk assurance activities are undertaken for all ICT systems and cyber security standards are maintained. The ABS is undertaking an IRAP assessment of TableBuilder to verify the security of all aspects of the implemented solution. The ABS is committed to act on the outcomes of the TableBuilder security

			assessment so that any risk of unapproved access to personal information is effectively managed from a IT security perspective. *Recommendation 4: Implement any outcomes arising from security assessments to assure the continued security of microdata in TableBuilder.* There are future plans to move TableBuilder infrastructure to cloud based services to further strengthen security. This will require additional review against the APPs. *Recommendation 5: Conduct a new PIA on the proposed TableBuilder move to cloud based services.*
APP12 – Access to personal information	Compliant	On request, the ABS can provide a TableBuilder user with details of the personal information we hold about them. Given this information is very limited, this is not likely to be a frequent request. The ABS will not charge for these requests.	APP12 requirements for microdata accessed by TableBuilder are consistent with the assessment described in the MADIP PIA Update.
APP13 – Correction of personal information	Compliant	The ABS has policies and procedures in place for complaints and the correction of inaccurate data. ABS staff responsible for administering TableBuilder can update their own personal information, and information about TableBuilder users, via the administrator user interface. TableBuilder users can update their own information or request this information be corrected. This is a regular occurrence already, particularly when machinery of government changes require the ABS to update email addresses for government users.	APP13 requirements for microdata in TableBuilder are consistent with the assessment described in the MADIP PIA update.

PART 4. ABS RESPONSE AND NEXT STEPS

In undertaking this PIA, the ABS has considered the current state of TableBuilder infrastructure, including user registration and subsequent storage of personal information, as well as the TableBuilder table population processes and recommended options for managing, minimising, or eliminating privacy impacts.

Based on the assessment against the Australian Privacy Principles (APP) (section 3) this PIA found the TableBuilder processes for collecting, storing and using the personal information of Users of TableBuilder to be compliant with eleven of the thirteen APPs, but with a best practice recommendation made to improve transparency around the management of User information. For two APPs (APP1, APP5), action is required to ensure transparency around the collection, use and disclosure of the personal information of Users as well as security of this information. The ABS is committed to implementing all recommendations for the management of TableBuilder.

The ABS is continuously improving data handling practices and infrastructure, including for TableBuilder, to preserve privacy, ensure data security, and increase data quality and utility. This PIA is a demonstration of the ABS' commitment to managing the privacy impacts of the project.

Appendix A – Acronyms

Acronym	Term
ABS	Australian Bureau of Statistics <www.abs.gov.au>
APP	Australian Privacy Principle
ASD	Australian Signals Directorate
EURS	External User Registration System
IRAP	Infosec Registered Assessors Program <https://www.cyber.gov.au/programs/irap>
ICT	Information and Communications Technology
MADIP	Multi-Agency Data Integration Project
OAIC	Office of the Australian Information Commissioner <www.oaic.gov.au>
PIA	Privacy Impact Assessment

Appendix B – Glossary

Term	Description
Administrative data	Data maintained by governments and other entities, including data used for registrations, transactions, and record keeping, usually during the delivery of a service.
Australian Privacy Principles	Principles contained in the *Privacy Act 1988* that regulate the way we collect, store, provide access to, use, and disclose personal information.
Registered users	As part of the safe people element of the Five Safes Framework, access to TableBuilder is provided to researchers who have registered as an individual or as a member of their organisation in the ABS Registration Centre, and agreed to the Conditions of use for TableBuilder.
Cloud	As per the US National Institute of Standards and Technology (NIST) definition of cloud computing.
Data Custodian	The agency that collects or generates data for any purpose and is accountable and responsible for the governance of that data.
De-identified	Personal information is de-identified 'if the information is no longer about an identifiable individual or an individual who is reasonably identifiable' (section 6(1) of the Privacy Act). (De-identified data is different to unidentified data - see the meaning of unidentified data.)
Five Safes Framework	An internationally recognised approach to managing disclosure risk – each 'safe' refers to an independent but related aspect of disclosure risk.
Microdata	Data in a unit record file that provides detailed information about people, households, businesses or other types of records.
Personal information	As defined in section 6(1) of the *Privacy Act 1988*.
Privacy Impact Assessment	A systematic assessment of a project that identifies the impact that it might have on the privacy of individuals, and sets out recommendations for managing, minimising, or eliminating that impact
Re-identification	The act of determining the identity of a person or organisation even though directly identifying information has been removed.
Sensitive information	As defined in section 6(1) of the *Privacy Act 1988*.
Unidentified	Data is considered 'unidentified' when direct identifiers such as name and address are removed or altered into an unidentifiable form. Further confidentialisation or safeguards (such as access controlled through the Five Safes Framework) are often required for the data to be considered de-identified.
Users	Registered researchers and ABS staff with access to TableBuilder

Appendix C – Registration Centre user functionality

1. External User - (individual)
    a. New user registration.
    b. User account activation.
    c. User forgot user id.
    d. User password reset.
    e. User details update.
    f. User password update.
    g. User secret question update.
    h. User product registration for individual licence.

2. External User - Organisation
    a. Organisation member
        i. View all available organisation access.
        ii. View all available contact officer.
        iii. Withdraw from organisation.

    b. Contact officer
        i. Update organisation details.
        ii. View all contact officer.
        iii. Remove contact officer.
        iv. View/download all organisation members.
        v. Remove member from organisation.
        vi. View all organisation users' available product access.

3. Registration Admin.
    a. User list for selected functional area.
    b. Find user by User ID or email address.
    c. Update user details.
    d. User password reset.
    e. List new registered user (User account not activated yet).
    f. List pending product registration.
    g. Finalise pending product registration.
    h. Create new organisation.
    i. Update organisation details.
    j. Organisation list.
    k. View available products for selected organisation.
    l. View organisation member list for selected organisation.
    m. Request products to be added to organisations
    n. Add user to organisation
    o. Remove user from organisation
    p. Add contact officer to organisation
    q. Remove contact officer from organisation
    r. Move users from one organisation to another organisation
    s. Set user to cancelled/inactive
    t. Set organisation to cancelled/inactive
    u. List all active and cancelled products for all organisations
    v. List all products
    w. List all active product access for all users

Appendix D – Application of the Five Safes Framework in the TableBuilder environment

Safe	Level of control	TableBuilder
Safe People	Some control	Users of TableBuilder must register to use the data and accept the Conditions of use. Breaches of protocols or disclosure of information may be subject to sanctions
Safe Projects	No control necessary	Any registered user can use the data for their own purposes.
Safe Settings	Very high control	TableBuilder requires secure log in by registered users and has auditing and monitoring capabilities, enabling the removal of user access where a user does not comply with the Conditions of use. Users do not have direct access to the microdata and all results produced from queries are in aggregate table form. TableBuilder populates all the tables through the same underlying data separation process. To do this all requests are submitted to the table queue. To minimise the risk of identifying individuals in aggregate statistics, a technique is applied to randomly adjust cell values, known as perturbation. This process has a negligible impact on the underlying pattern of the statistics while avoiding the release of identifiable data.
Safe Data	High control	The microdata accessed by TableBuilder is unidentified data used to produce tabular output. It is treated by the ABS, prior to access by TableBuilder to reduce the risk of re-identification of the information. All microdata accessed by TableBuilder is carefully prepared to ensure that it is not likely that individuals are able to be identified including, removal of direct indentifiers. Users do not have direct access to the microdata and all results produced from tables submitted in TableBuilder are in aggregate form.
Safe Outputs	Very high control	Every table produced through TableBuilder is aggregated data. All tables are submitted to a table queue to separate users from unit record data. To maintain the confidentiality of respondents and reduce the risk of re-identification TableBuilder has some system restrictions in place, including: • not allowing users to download individual records • perturbing output in tables • preventing cross-tabulation of certain variables. The ABS provides guidelines and rules about what may be published or shared. Breaches of protocols or disclosure of information may be subject to sanctions and/or legal proceedings