Australian Government
Australian Public Service Commission

Privacy Impact Assessment:
Bespoke Surveys
October 2020

Conducted by:	Workforce Research and Analysis
Director:	Dr Nicole Steele
Conducted on:	October 2020
Project Name:	Strategic Policy and Research Group Bespoke surveys

Threshold Assessment Report

Brief description and overall aims of project:

Strategic Policy and Research Group (SPRG) administers bespoke surveys to support Groups internal to the Australian Public Service Commission (APSC). More rarely, SPRG administers surveys on behalf of other APS agencies.

Bespoke surveys provide insight into APS workplaces and results are used to inform workforce strategies. All Groups and APS agencies (referred to throughout as the sponsors of the surveys) are required to adhere to the Australian Privacy Principles (APPs).

Brief description / nature / sensitivity of any personal information that will be collected, used, or disclosed:

Most bespoke surveys do not require respondents to provide their names or other explicitly identifying information, such as AGS number. However, it is possible for respondents to provide unsolicited personal information about themselves or others in free-text response items. In some cases, it may also be possible to infer a respondents' identity from the demographic and organisational information they provide. While it varies, the data collected within bespoke surveys can include:

- Demographic information such as gender, age, Indigenous status, disability status, and educational qualifications;
- Organisational information such as agency and/or work unit; and
- Opinions and attitudes on issues including, but not limited to, employee engagement, leadership, job satisfaction and general impressions of the APS.

If this is an existing project, list any planned modifications to the way personal information will be handled:

When this Threshold Assessment was first undertaken (2017), the platform to administer surveys was Checkbox survey software. Since 2020, surveys are run through Microsoft Forms or Qualtrics.

Please list any view of stakeholders about the impact of the project on information privacy:

The key stakeholders for this programme are SPRG and the sponsors on whose behalf the surveys are administered. Due to the ad hoc nature of these surveys, no specific views have been sought during the completion of this PIA. However, some generalisations can be made:

- Sponsors are supportive of SPRG taking all necessary steps to protect the privacy of respondents before the data is provided to them.
- Sponsors agree to the appropriate handling and storage of survey data in accordance with privacy legislation when requesting SPRG to administer surveys.

If there have been no changes to personal information handling practices, describe how privacy risks are currently assessed and managed:

Privacy risks are managed in two ways:

- Management of the data
    - Data are securely stored with limited access (and only by trained personnel)
    - Prior to release of data to internal or external stakeholders, the privacy risks of releasing the data are assessed. Data are appropriately manipulated and de-identified to remove the risk that responses may be attributed to specific individuals

- Effective processes to safeguard the release of data to agencies
  - Access to the data is governed by formal guidelines
  - Data are provided only to the stakeholders who commissioned the survey
  - Data are released under caveats and the express agreement of sponsors to safeguard the privacy of individuals.

Threshold Assessment (please click on the appropriate boxes):

1. Will any personal information be collected, stored, used or disclosed in the project?	☒ Yes ☐ No (No PIA required)
2. If yes, does the project propose any changes to existing information handling procedures?	☐ Yes (Conduct PIA) ☒ No
3. If no, have the privacy implications of these practices been assessed previously?	☒ Yes ☐ No (Conduct PIA)
4. If yes, are current controls working?	☒ Yes ☐ No (Conduct PIA)

A Privacy Impact Assessment is required: ☒ Yes ☐ No

Assessment of High Risk

Does the project involve any of the following (please click all that apply):

☒ Material change to existing policies, processes or systems that involve personal information.

☐ The establishment of a new way of identifying individuals, such as a unique identifier, biometrics or online identification system.

☒ A material difference in the collection of, or the method of collection of, new or changed types of personal information.

☒ The collection of sensitive information.

☐ The use or disclosure of personal information for a purpose other than the purpose for which it was collected.

☒ Data matching or the bulk transfer of data.

☐ The transfer of personal information to an overseas recipient.

☐ A changed, or new, risk of misuse, interference and loss, or unauthorised access, modification or disclosure of personal information.

☐ The agency considers that the project involves such sensitivity, or is of such significance, that it constitutes a high risk project.

☐ The agency considers that the project is a high risk project for one of the above reasons or any other reason relating to privacy.

If you have checked the box for any of the above, **the APSC must publish (i) a PIA report and (ii) our response to the report recommendations on the APSC website**, unless publication would (please check all that apply):

☐ Unreasonably reveal information about an agency's systems, process or operations.

☐ Involve unlawful or unreasonable disclosure of personal information about any individual.

☐ Unreasonably reveal information about law enforcement or national security activities

☐ Involve the disclosure of an exempt document for the purposes of the *Freedom of Information Act 1982*

If it is not possible publish the PIA report or our response, **the APSC must publish a summary version or edited copy**, from which any information of the kinds specified on the left must be deleted (check one option below).

☐ Full PIA report and responses will be published on the APSC website.

☐ An edited or summary version will be published on the APSC website.

☒ The project is **NOT** deemed high risk and no report is required.

Privacy Impact Assessment Report (PIA)

1. Brief description and overall aims of project:

The Australian Public Service Commission (APSC) is a non-corporate Commonwealth entity. Statutory responsibilities are detailed in the *Public Service Act 1999* and require the APSC to:

- develop, promote, review and evaluate APS employment policies and practices
- facilitate continuous improvement in people management throughout the APS
- contribute to learning and development and career management
- contribute to and foster leadership in the APS
- provide advice and assistance on public service matters to entities
- promote high standards of integrity and conduct in the APS.

In order to fulfil these responsibilities, the Workforce Research and Analysis (WR&A) team within the Strategic Policy and Research Group (SPRG) administers bespoke surveys to support Groups internal to the APSC. Infrequently, SPRG administers surveys on behalf of other APS agencies.

Surveys are administered through Microsoft Forms and/or Qualtrics.

Bespoke surveys provide insight into APS workplaces and results are used to inform workforce strategies and facilitate continuous improvement in people management throughout the APS.

All Groups and APS agencies (referred to throughout as the sponsors of the surveys) are required to adhere to the Australian Privacy Principles (APP).

a. How do these aims fit with the APSC's broader objectives?

The aims of these surveys are aligned with the statutory responsibilities of the APSC under the Public Service Act (1999) (see above). They are designed to:

- Develop, promote, review and evaluate APS employment policies and practices
- Facilitate continuous improvement in people management throughout the APS
- Provide advice and assistance on public service matters to entities

b. What is the project's scope and extent?

The scope and extent of bespoke surveys are defined by the sponsor. Surveys may be administered to respondents within an entire agency or subgroups of the workforce. The length and topic of surveys also varies according to the sponsors' need.

c. List any links with existing programs or other projects:

By their ad hoc nature, bespoke surveys may be linked to a range of existing programs or other projects. This includes project and programme evaluations and ongoing policy work in the APSC and broader APS.

d. Who is responsible for the project?

The WR&A team in SPRG of the APSC.

e. What is the timeframe for decision-making that will affect the project's design?

N/A

f. Brief description of the key privacy elements (e.g., extent and type of information that will be collected, how security and information quality will be addressed, how information will be used and disclosed)

The bespoke surveys are fully compliant with the APSC's privacy policy, which sets out the kinds of information collected and held; how this information is collected and held; its purposes; and authority for its collection. The full APSC privacy policy is available at www.apsc.gov.au/Privacy.

Collection: Personal information such as age, gender, or workplace location may be collected. Sensitive information may also be requested of a respondent.

Workplace email addresses are used to send respondents survey links. Where generic survey links are used, these addresses are not linked to survey responses. Where a tailored survey link is supplied to individual respondents, their email address is removed and destroyed when the survey administration period closes.

Usage: Most data are disclosed in aggregated tables. Unit record data are only released under very strict conditions, and never publically published.

Security: The bespoke surveys have password-protected storage and limited access only - by trained WR&A staff. Only the WR&A team have access to the live, underlying data when surveys are 'open' in the field.

2. Identifying and consulting stakeholders

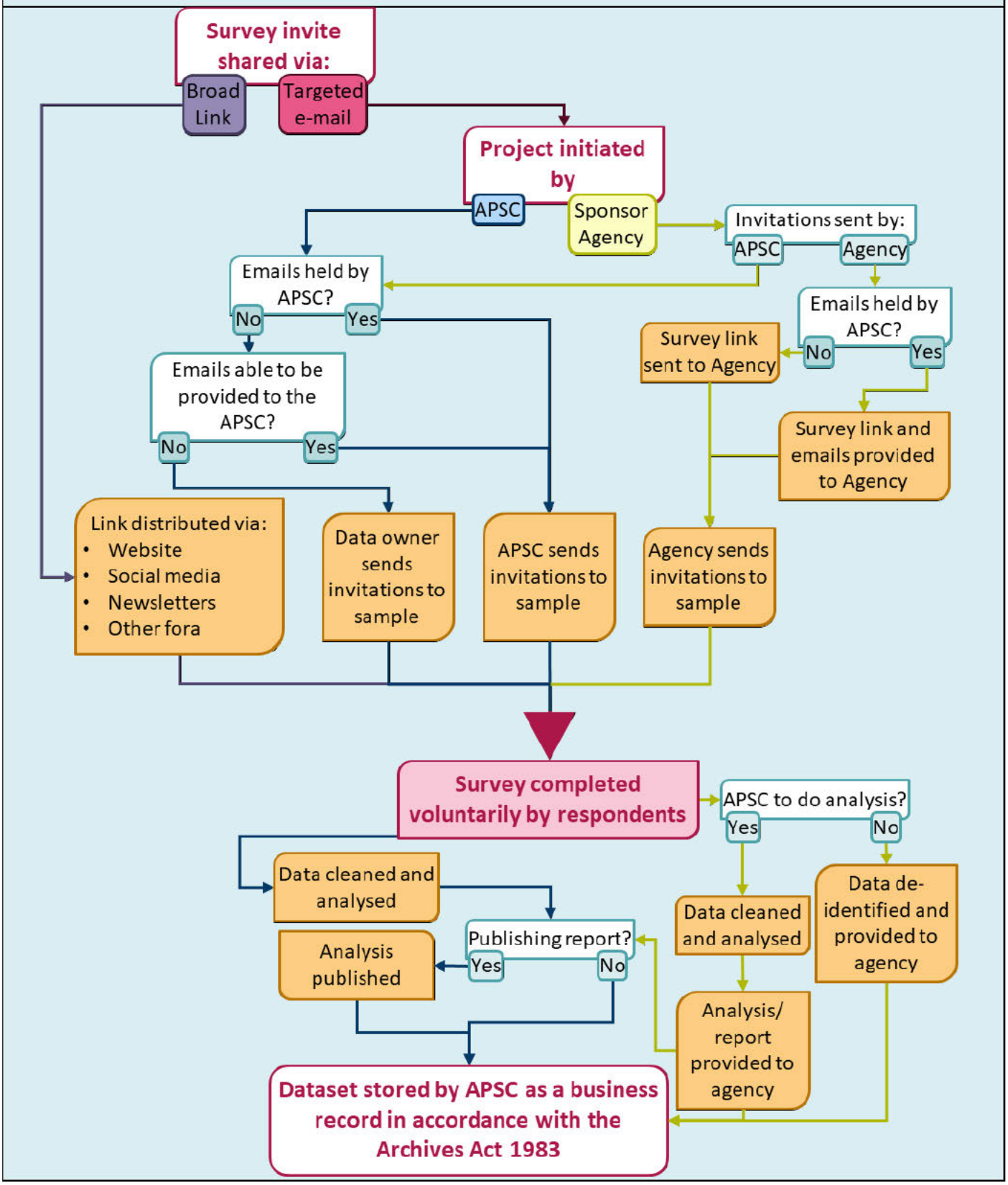
a. List the project's **internal** stakeholders and whether they will be consulted (e.g., data subjects, data requesters):

- General Counsel, Integrity, Performance and Employment Policy Group – the General Counsel is often consulted on privacy matters and has been consulted on the development of the original PIA.
- APSC Groups on whose behalf bespoke surveys are administered. The process for requesting a bespoke survey and subsequent data ensures the privacy obligations of SPRG and the requesting group are explicitly stated.
- SPRG - All SPRG staff developing, administering, and reporting on the bespoke survey data are trained to follow standard operating procedures in the access and use of these datasets.

b. List the project's **external** stakeholders and whether they will be consulted (e.g., data subjects, data requesters, regulatory authorities, advocacy organisations, service providers, industry experts, academics):

- APS agencies on whose behalf bespoke surveys are administered. APS agencies are consulted at the time of request. The process for requesting bespoke survey administration and data ensures the privacy obligations of SPRG and the requesting agency, outlined in the PIA, are explicitly stated.

3. Map information flows



a. Identity verification:
   - Can anonymous or de-identified information be used?
   - Must identities be verified? If so, how?
   - Are identification numbers needed? Could they be used for other purposes? What protections will prevent other uses or adoptions?
   - What other information may need to be verified?

- Can anonymous or de-identified information be used?
- Must identities be verified? If so, how?

The bespoke surveys do not request identifying information such as Australian Government Service (AGS) numbers or names. Where respondents provide demographic information, this is provided and assumed to be correct. No attempt is made to verify this information. If respondents identify themselves in free-text questions this information is subsequently redacted before providing data to sponsors.

If surveys are administered through individual email links then a respondent's email address will be attached to his/her responses. At the close of each survey, the WR&A team within SPRG removes these email addresses when exporting the survey responses, and destroys this information.

- Are identification numbers needed? Could they be used for other purposes? What protections will prevent other uses or adoptions?

Identification numbers are not used in bespoke surveys beyond those automatically generated by survey software.

b. Information collection:
   - What personal information will be collected, which of it is sensitive?
   - Why is this information necessary?
   - Can it be collected in a de-identified or anonymous way?
   - Can individuals choose not to provide some or all of the personal information?
   - Is the collection method reasonably unobtrusive, potentially sensitive, covert, or intrusive?
   - How, where, and by whom will it be collected?
   - Will unsolicited personal information be used?
   - How will an individual's circumstances be taken into account during collection?
   - Is there any legislation or other authority which you rely on to collect?
   - What collection alternatives have been considered and rejected?
   - How often will personal information be collected (e.g., once only, periodically, ongoing?)
   - Are there limits on the nature of the information to be collected?
   - What and how will collection information be given to the individual?

Personal data. Most bespoke surveys do not require respondents to provide their names or other explicitly identifying information, such as AGS number. However, it is possible for respondents to provide unsolicited personal information about themselves or others in free-text response items. In some cases, it may also be possible to infer a respondents' identity from the demographic and organizational information they provide. While it varies, the data collected within bespoke surveys can include:

- Demographic information such as gender, age, Indigenous status, disability status, and educational qualifications;
- Organisational information such as agency and/or work unit; and
- Opinions and attitudes on issues including, but not limited to, engagement, leadership, job satisfaction and general impressions of the APS.

If a bespoke survey is administered through a tailored link, then an individual's email address is collected and attached to his/her survey responses. All respondents are advised of this before commencing the survey. They are also advised of the procedures SPRG takes at the close of the survey to separate the email addresses from survey responses, and delete this personal information.

Sensitive data. Under the Privacy Act (1988), sensitive data are a subset of personal information which is generally afforded a higher level of protection under the APPs. Bespoke surveys generally do not collect sensitive information, however it is possible for a sponsor to request the collection of information such as:

- racial or ethnic origin
- sexual orientation
- health information.

Information collection. This information may be used to inform workplace policies and practices, such as those related to identified diversity groups. The aims of these surveys are aligned with the statutory responsibilities of the APSC under the *Public Service Act 1999* (see Section 1 above). They are designed to:

- Develop, promote, review and evaluate APS employment policies and practices
- Facilitate continuous improvement in people management throughout the APS
- Provide advice and assistance on public service m
- atters to entities

Survey data are collected through Qualtrics or Microsoft Forms software via either a tailored survey link or a generic link. WR&A team prepare the survey in consultation with the sponsor.

Respondents' ability to access their responses depends on the style of administration:

- For bespoke surveys with unique survey links, a respondent can gain access to his/her responses during the survey administration period by logging back in.
- For bespoke surveys administered through a general survey link, no identifying details are collected with the individual's data. The individual cannot gain access to his/her responses.

Bespoke surveys often include free-text questions that allow participants to provide written responses. Participants may provide unsolicited personal information, such as the name of a colleague or supervisor. The WR&A team within SPRG does not use any unsolicited personal information in research or reporting. Furthermore, all free-text responses are screened and unsolicited personal information is redacted before data are provided to sponsors.

c. Information use:
- What are all the planned uses of the personal information?
- How do all these uses relate to the purpose of collection?
- What measures prevent uses for secondary purposes?
- What measures ensure secondary uses are permitted?
  i. Is consent required for secondary use?
  ii. Is the secondary use related to the purpose of collection?
  iii. Can an individual refuse consent for secondary use and still be involved in the project?
  iv. How can individuals be involved in decisions about new, unplanned purposes that occur during the project?
- Does your project involve data linking or matching?
  i. How might this be done?
  ii. What decisions affecting the individual might be made on the basis of data-linking or matching?
  iii. What safeguards will limit inappropriate access, use and disclosure of linked information?
  iv. Outline audit trails and other oversight mechanisms.
  v. How will data linkage accuracy be ensured?
  vi. How will individuals be protected from the adverse effects of incorrect data matching?

The purpose of collecting personal information is to enable a more detailed/thorough exploration of results, to determine if there are differences across subgroups (e.g. gender, classification level, ongoing/non-ongoing). This information is then used to tailor policies and programs, or develop targeted interventions if required.

To date there have been no secondary uses of bespoke survey data. Bespoke surveys are tailored specifically to the project. In future, should a secondary use of bespoke data occur then individuals could not consent, or refuse consent, to any potential secondary use because there are no identifying information linking survey responses to individuals.

Individual-level data from bespoke surveys are not matched to other datasets.

d. Information disclosure:
- How, to whom and why will it be disclosed?
- Will disclosed information have the same privacy protections after disclosure?
- Will the information be published, or disclosed to a register?
- Will individuals be told about disclosure or given choices about disclosures?
- Is disclosure authorised or required by law? If so, which laws?
- Will the personal information be disclosed to overseas recipients?

Data are disclosed in two formats:

- Aggregated data are published in internal or external reports. These may be applied for under the *Freedom of Information Act (FOI) 1982*.
- Datasets are disclosed to the sponsors of the surveys. This includes other internal APSC groups or APS agencies after consultation and negotiation, and completion of a risk management process.

These datasets are released under the proviso that:

- Only aggregated data will be published
- The recipient will not attempt to re-identify individuals

- The dataset will be stored securely and destroyed after the recipient's current project is completed.

Individuals are provided with information on how their data will be disclosed. Based on this information they can opt to complete or not complete the survey.

Complete datasets are stored securely on the APSC servers and are only accessible by SPRG employees. Where data are provided back to agencies, appropriate storage is their responsibility.

All information published by SPRG in the form of research notes or requests for information are recorded on internal SPRG registers.

SPRG does not disclose personal information from bespoke surveys to overseas recipients.

e. Information quality:
   - What are the processes for ensuring only relevant, up-to-date and complete information is used or disclosed?
   - How will personal information updates be given to previous data users?
   - What are the consequences for individuals if personal information is not accurate or up-to-date?

Before developing a bespoke survey, the WR&A team within SPRG consults with the sponsor to ensure that the data collected is relevant and necessary.

No updates to personal information are required given that each bespoke survey reflects a specific point in time. As such, there are no consequences to the bespoke project if a respondent's personal information changes over time.

f. Information security:
   - What security measures and systems will protect the information from loss, unauthorised access, use, modification, disclosure or other misuse (including for contracted service providers)? How will it be protected if managed by someone else?
   - How will information be transferred between sites?
   - Who will have access to it? Who will authorise access?
   - What action will be taken if there is a data breach?

Data from each bespoke survey are stored on APSC servers administered by the Department of Prime Minister and Cabinet (PM&C).

Where de-identified data needs to be transferred, this is done by email through the protected network to reduce the potential for data to be lost in transit. Appropriate storage of the data is the responsibility of the receiver.

A comprehensive staff training and awareness program has been developed to ensure all personnel are fully aware of their information security responsibilities. This includes compliance to internal data handling procedures.

Furthermore, in order to comply with the OAIC's Data Breach Notification Scheme a breach protocol has been developed to enable rapid response to any potential data breach.

Microsoft Forms:

The Department of Finance has undertaken an IRAP assessment of GovTEAMS and accredited the system to hold information up to and including the OFFICIAL: Sensitive classification. Finance undertakes a risk-based approach to ICT Security, including Cloud Security. Finance follows Commonwealth Government Guidelines as laid out in the Information Security Manual https://acsc.gov.au/infosec/ism/

Qualtrics:

Qualtrics' in-house Security Operations Center monitors the confidentiality, integrity, availability and performance of data with sophisticated intrusion detection systems, performance and health systems, and security event correlation systems.

https://www.qualtrics.com/au/platform/security/?rid=ip&prevsite=en&newsite=au&geo=AU&geomatch=au

g. Retention and destruction:
- How will personal information be de-identified or securely destroyed?
- Do you have an information retention policy and destruction schedule?
- How will compliance with this policy and any relevant legislation about record destruction be assessed?

Data from bespoke surveys are retained as a business record on Sharehub (the internal APSC electronic document and records management system – EDRMS) and may be destroyed after 7 years after action is complete in accordance with APSC's Records Authority. These practices are consistent with the Archives Act (1983).

h. Access and correction:
- What ability will individuals have to access and correct their personal information and what will it cost them?
- How will decision be made about requests from individuals for access to, or correction of, their information?

If a tailored survey link is used to administer a bespoke survey, then an individual can contact the WR&A team during the time a survey is open in the field to correct any information, or to clear all their responses. This is completed free of charge. Once a survey closes, this email identifier is removed and destroyed. Respondents are advised of this before completing the survey.

Other bespoke surveys are administered through a general survey link. As such, no identifying details are collected with the individual's data. Individuals cannot access and/or correct their information.

4.	Privacy impact analysis and compliance check

a. APP1 – Open and Transparent Management of Personal Information (Ensures that APP entities manage personal information in an open and transparent way. This includes having a clearly expressed and up-to-date APP privacy policy).

- Have reasonable steps been taken to implement practices, procedures, and systems that will ensure compliance with the APPs and any binding registered APP code?
- Do you have an APP Privacy Policy which:
  - i. Is clearly expressed and up-to-date?
  - ii. Covers: (i) the kinds of personal information collected and held; (ii) how the information is collected and held; (iii) the purposes for which the information is collected, held, used and disclosed; (iv) how individuals may access their information; (v) how individuals may complain about privacy breaches and how the APSC deals with complaints; (vi) the likelihood of personal information being disclosed to overseas recipients; (vii) which countries of residence information overseas recipients are likely to be located in?
  - iii. Is freely available at no cost (e.g., on your website)?
- Have reasonable steps been taken to ensure that procedures and systems are in place for handling privacy inquiries and complaints?

The APSC Privacy Policy complies with APP1. The APSC has an up-to-date APP privacy policy, including the handling of complaints and breaches, which is published on their website: http://www.apsc.gov.au/Privacy

All bespoke surveys are conducted under a collection statement that explains to respondents how the data they provide will be stored and used. This includes providing contact details allowing individuals to contact the APSC for further information, clarification or to provide comment.

b. APP2 – Anonymity and Pseudonymity (Requires APP entities to give individuals the option of not identifying themselves, or of using a pseudonym. Limited exceptions apply).

- Will individuals have the option of not identifying themselves or of using a pseudonym when participating in the project?
- Exception: Are you required or authorised by or under an Australian law, or a court/tribunal order, to deal with individuals who have identified themselves?
- Exception: Is it impracticable for you to deal with individuals who have not identified themselves or who have used a pseudonym?
- Are there categories of individuals affected by the project who are likely to seek to interact with your agency or organisation anonymously or using a pseudonym?

Bespoke surveys are anonymous by default. These surveys do not collect specific identifying information such as name, date of birth, or AGS number.

There is one exception to this: when a bespoke survey link is tailored and sent to individual respondents. Respondents are advised before commencing the survey that their email address will be linked to their responses until the close of the survey, at which time it will be destroyed. Respondents can opt to not complete the survey.

c. APP 3 — Collection of Solicited Personal Information (Outlines when an APP entity can collect personal information that is solicited. It applies higher standards to the collection of 'sensitive' information).

- Personal information:
  - i. If you are an agency, is the information being collected necessary for or directly related to one or more of your functions?
  - ii. If you are an organisation, is the information being collected necessary for one or more of your functions?
  - iii. Is the collection authorised or required by an Australian law or a court/tribunal order?
  - iv. Will the information be collected by lawful and fair means?
  - v. Will the personal information be collected directly from the individual concerned? If not, do any of the exceptions in APP 3.6 apply: (a) the individual consents; (b) required by law; (c) unreasonable or impracticable to do so?
- Sensitive information:
  - i. Can you rely on any of the exceptions in APP 3.3 or APP 3.4 for the collection of sensitive information?
    1. APP 3.3 Exceptions: (a) individual consented; and (b) information is reasonably necessary or directly related to the entity's functions?
    2. APP 3.4 Exceptions: (a) required or authorised by law; (b) a permitted general or health situation[1]; (c) law enforcement; (d) non-profit member / client information.
  - ii. Will there be guidance or processes in place to assist with the handling of sensitive information?
  - iii. If the collection and management of sensitive information will be outsourced, will measures be in place to protect the sensitive information and will compliance with APP 3 be monitored?

At times, there may be questions in bespoke surveys that are considered 'sensitive' as per the Office of the Australian Information Commissioner APP Guidelines. This can include questions on:

- racial or ethnic origin
- sexual orientation or practices
- health information about an individual.

All personal and sensitive information collected in bespoke surveys is necessary to allow the experiences of different subgroups to be explored. This may include looking at whether current practices have systematically different impacts on certain groups such as women or Aboriginal/Torres Strait Islander (ATSI) employees. Collecting this information is part of the APSCs role under the Public Service Act (1999) outlined in Section 1 of this PIA.

Furthermore, unless of critical importance to the activity, data collections, including personal and sensitive information, are voluntary. Where individuals do not wish to provide this information they may skip questions, or select a 'Choose not to respond' option. Where questions are mandatory and require a response in order for the employee to submit a valid response to the survey, this is explained to respondents prior to commencing the survey.

The de-identified nature of bespoke surveys, coupled with the secure storage and limited distribution of data, minimises the likelihood that sensitive information may be used inappropriately.

[1] A ***general situation*** includes: serious threat to life or safety; action against criminal activity; missing persons; legal claims; dispute resolution; diplomatic functions; Defence Force activities.

d. APP 4 — Dealing with Unsolicited Personal Information
   - Are there practices, procedures, and systems in place for dealing with the receipt of unsolicited personal information that will ensure compliance with APP 4?

Bespoke surveys often include free-text questions that allow participants to provide written responses. Participants may provide unsolicited personal information, such as the name of a colleague or supervisor. The WR&A team within SPRG does not use any unsolicited personal information in research or reporting. Furthermore, all free-text responses are screened and unsolicited personal information is redacted before data are provided to sponsors.

e. APP 5 — Notification of the Collection of Personal Information (Outlines when and in what circumstances an APP entity that collects personal information must notify an individual of certain matters):
   i. The APP entity's identity and contact details
   ii. The fact and circumstances of collection
   iii. Whether the collection is required or authorised by law
   iv. The purposes of collection
   v. The consequences if personal information is not collected
   vi. The APP entity's usual disclosures of personal information of the kind collected by the entity
   vii. Information about the APP entity's APP Privacy Policy
   viii. Whether the APP entity is likely to disclose personal information to overseas recipients, and if practicable, the countries where they are located.
   - Consider each of the matters listed above. Will steps be taken to notify the individual of each matter? If steps are not being taken in relation to a matter, is it reasonable in the circumstances not to notify the individual?
   - Are practices, procedures, and systems in place to ensure reasonable steps are taken to tell the individual about the matters listed above at or before (or if not practicable, as soon as practicable after) the time of collection?
   - If the information is collected directly from the individual, will notice be given to the individual (such as by displaying the notice on a form, providing a link on a web page or advising the individual over the phone) and the individual asked to confirm they have been notified of the APP 5 matters before providing their personal information?

Bespoke survey collection notices comply with the requirements outlined in APP 5. While tailored to each survey, information covered includes:

- Who is collecting the personal information
- Why the Commission collects personal information
- Who the Commission discloses the personal information to

The collection notice is available at the beginning of all bespoke surveys. This informs the respondent of all of the above issues as well as providing a point of contact within SPRG to seek further information or clarification. Respondents can then make an informed choice as to whether they wish to provide their data.

f. APP 6 — Use or Disclosure of Personal Information (Outlines the circumstances in which an APP entity may use or disclose personal information that it holds).

- If the use or disclosure is for a secondary purpose, will the individual be asked to provide consent? Will you keep a record of the consent?
- If the individual will not be asked to consent, do any of the other exceptions to the requirement for consent in APP 6.2 apply: (a) individual would reasonably expect disclosure; (b) secondary purpose is directly related to primary purpose; (c) required or authorised under law; (d) permitted general or health situation?
- If you are an agency, is it possible that personal information may be used or disclosed because it is reasonably necessary for an enforcement related activity? If so, are procedures in place to ensure a written note of the use or disclosure is made?

Under APP 6, an entity can only use or disclose personal information for a purpose for which it was collected (known as the 'primary purpose'), or for a secondary purpose if an exception applies. The exceptions include:

- the individual has consented to a secondary use or disclosure
- the individual would reasonably expect the use or disclose their personal information for the secondary purpose, and that purpose is related to the primary purpose of collection, or, in the case of sensitive information, directly related to the primary purpose

Use and distribution of data from all bespoke surveys are governed by these principles.

The collection statement for these surveys varies with each administration, but informs the respondents of the purpose and use of the data being collected. To date, data collected in these surveys have not had secondary uses. However, if a secondary purpose is foreseen, then the collection statement will be modified to include secondary use or disclosure where appropriate. By providing respondents with this information, they are able to make an informed choice as to whether they provide information based on its intended primary and potential secondary uses.

The collection statement also clarifies if information/data will be returned to the sponsor for internal use. By completing the surveys, respondents are considered to have consented to this use and distribution of their personal data.

g. APP 7 — Direct marketing (An organisation may only use or disclose personal information for direct marketing purposes if certain conditions are met).

- Do any of the exceptions permitting the use or disclosure of personal information for the purpose of direct marketing as set out in APP 7.2 or APP 7.3 apply: (a) organisation collected the information; and (b) individual would reasonably expect disclosure; and (c) organisation offers simple means to opt out in all direct marketing communications; and (d) individual has not opted out; (e) information provided by someone other than individual; (f) consent is impracticable?
- If sensitive information is to be used or disclosed for the purpose of direct marketing, will the individual be asked to consent?
- An organisation may use or disclose personal information if contracted by the Commonwealth Govt for collection purposes. If you are a contracted service provider for a Commonwealth contract, is the use or disclosure necessary to meet an obligation under the contract?
- If use or disclosure of personal information for the purpose of direct marketing is permitted under APP 7, will individuals be given the opportunity to request not to receive direct marketing communications?
- Does your organisation have any guidance or processes in place to help manage your direct marketing obligations?
- Have you considered your obligations under the Do Not Call Register Act 2006 and the Spam *Act 2003*?

As a non-commercial entity, the APSC is exempt from consideration of APP7. However, there is no use or disclosure of any personal information collected for direct marketing purposes.

h. APP 8 — Cross-border Disclosure of Personal Information (Outlines the steps an APP entity must take to protect personal information before it is disclosed overseas).

- *An APP entity that discloses personal information to an overseas recipient **is accountable for any acts or practices of the overseas recipient** in relation to the information that would breach the APPs.*
- If personal information is to be disclosed to an overseas recipient, will reasonable steps be taken to ensure the overseas recipient does not breach the APPs (other than APP 1) in relation to the information?
- Do any of the following exceptions apply:
  i. (a) Reasonable expectation that recipient is subject to a law or binding scheme equivalent to the APPs; and (b) mechanisms exists that an individual can access to enforce that equivalent law or binding scheme?
  ii. (a) The organisation expressly informs individuals that APP 8 will not apply; and (b) individual still consents?
  iii. Required or authorised under law?
  iv. A permitted general situation
  v. An agency is required or authorised under an international agreement?
  vi. Law enforcement?
- If no exception applies, are appropriate arrangements in place with overseas recipients to ensure that personal information is handled in accordance with the APPs?

All data are collected on behalf of internal APSC Groups or APS agencies. When bespoke survey data are provided to agencies, it does not cross-borders. Bespoke survey data are not provided by the APSC to overseas recipients.

i. APP 9 — Adoption, Use or Disclosure of Government-related Identifiers (Outlines the limited circumstances when an organisation may adopt a government-related identifier of an individual as its own identifier, or use or disclose a government related identifier of an individual).

- *An organisation* must *not adopt, use or disclose a government-related identifier of an individual as its own identifier of the individual unless an exception applies.*
- Do any of the following exceptions apply:
  i. Reasonably necessary to verify individuals for purposes of organisation's functions?
  ii. Reasonably necessary to fulfil obligations to agency or State / Territory authority?
  iii. Required or authorised by law?
  iv. Permitted general situation?
  v. Law enforcement?
  vi. Prescribed by regulation?
- Is any planned adoption, use, or disclosure of government related identifiers permitted under an exception in APP 9?

Bespoke surveys do not use government-related identifiers.

If a tailored survey link is used to administer surveys, a respondent's email is removed and destroyed at the completion of the survey administration period.

j. APP 10 — Quality of Personal Information (Requires personal information collected, used, and disclosed is accurate, up-to-date, and complete).

- Will reasonable steps be taken to ensure that any personal information collected is accurate, up-to-date and complete? Will guidance or processes be in place to ensure these steps are followed?
- Will reasonable steps be taken to ensure that any personal information being used or disclosed is accurate, current, complete and relevant, having regard to the purpose of the use or disclosure? Will guidance or processes be in place to ensure these steps are followed?

The purpose of bespoke surveys is to collect information at a specified point in time. As such, there is no requirement or need to ensure personal information is kept up to date. There is no risk to the individual or to the project if personal information changes over time.

Furthermore, because of the anonymous nature of bespoke surveys it is not possible to check the accuracy of individual survey responses against other sources of information, such as administrative data, to ensure the personal information collected is accurate.

k. APP 11 — security of personal information (requires personal information is protected from misuse, interference, loss unauthorised access, modification or disclosure and is correctly destroyed).

- Will reasonable steps be taken to ensure that the personal information to be collected is protected from unauthorised access, modification, or disclosure?
- Consider whether reasonable steps will be taken to ensure technical and physical security is in place to protect against misuse, interference, and loss, and whether there will be technical and physical security guidance/processes in place.
- Will control procedures be in place requiring authorisation before personal information is added, changed, or deleted?
- Will audit mechanisms identify inappropriate system access?
- Will reasonable steps be taken to destroy or de-identify the personal information which is no longer needed for any authorised purpose?
- If reasonable steps will not be taken to destroy or de-identify the personal information which is no longer needed for any authorised purpose, do any of the exceptions apply:
  i. Information is part of a Commonwealth record?
  ii. Is APP entity required by law or a court/tribunal order to retain?
- Will guidance or processes be in place to help determine when and how destruction or de-identification of personal information will occur?
- Is staff training adequate to fulfil the reasonable steps required?

The following steps have been taken to ensure the security and protection of bespoke survey data:

- The de-identified datasets are stored on PM&C servers and all computers are password protected. They are also stored as records within Sharehub, the APSC's internal EDRMS.
- Only the WR&A team in SPRG has access to the full datasets.
- Datasets are write-protected so that they cannot be accidently modified. Personal information cannot be added, changed, or deleted.
- SPRG staff are trained to follow standard operating procedures in the access and use of these datasets.

The following audit mechanisms are applied:

- Internal and external data users must apply for the data through the completion of a data request and privacy risk analysis form.
- The responsible SPRG officer also completes a privacy risk determination form outlining their assessment of the risk and steps taken to protect individuals' privacy.
- All requests and data releases are logged.

After use, data from bespoke surveys are stored and destroyed in accordance with the *Archives Act 1983*.

l. APP 12 — Access to Personal Information (Outlines an APP entity's obligations when an individual requests to be given access to personal information held about them by the entity. This includes a requirement to provide access unless a specific exception applies).

- Do any of the following exceptions apply:
  i. Agency is required or authorised to refuse under (i) FOI; (ii) any other Commonwealth Act
  ii. Organisation believes: (i) threat to life or safety; (ii) unreasonably impact other individuals; (iii) frivolous or vexatious; (iv) pertains to legal proceedings; (v) prejudice negotiations with individual; (vi) unlawful; (vii) does not comply with law or court order; (viii) would prejudice action against unlawful conduct; (ix) would prejudice law enforcement; (x) reveal commercial in-confidence information.
- Will processes be put in place to:
  i. Generally provide an individual with access to information being held about them?
  ii. Deal with requests for access within the appropriate time (for agencies, 30 days; for organisations, within a reasonable period after the request is made)?
  iii. Give access in the manner requested, if reasonable and practicable?
  iv. Negotiate and provide other reasonable means of access where a request is refused?
  v. Ensure agencies do not charge individuals for access to their information?
  vi. Ensure organisations do not charge excessively?
  vii. Ensure a written notice is given to an individual whose access request is refused, outlining: (a) reasons for refusal (where reasonable), (b) complaint mechanisms, (c) related regulatory matters?
- Will individuals be made aware of how to access their personal information?

Bespoke surveys are anonymous by default. These surveys do not collect specific identifying information such as name, date of birth, or AGS number.

If a tailored survey link is used to administer a bespoke survey, then an individual can contact the WR&A team during the time a survey is open in the field to access their information. This access is provided free of charge. Once a survey closes, this email identifier is removed and destroyed. Respondents are advised of this before completing the survey.

Most bespoke surveys are administered through a general survey link. As such, no identifying details are collected and linked to the individual's data. Individuals cannot access their information.

m. APP 13 — Correction of Personal Information

- This requirement applies where:
  i. The APP entity is satisfied the information is inaccurate, out-of-date, incomplete, irrelevant or misleading, having regard to a purpose for which it is held, or
  ii. The individual requests the entity to correct the information.
- Will individuals be made aware of how to request correction of their personal information?
- Will reasonable steps be taken to correct information that is not accurate, out of date, incomplete, irrelevant, or misleading, having regard to the purpose for which the information is held?
- Are processes in place for responding to requests from individuals to correct personal information?
- Are processes in place for identifying and correcting personal information that is inaccurate, out of date, incomplete, irrelevant, or misleading?
- Will individuals be informed about the reasons if a request for correction is denied?
- Are processes in place for associating a statement with personal information if a request for correction is denied?

Data from bespoke surveys are intended to reflect a specific point of time. There is no need to correct or update personal information should it change over time.

5. Risk Management Plan – identify any relevant risks and mitigation strategies. Modify, add, or delete risks and mitigations as necessary. Select likelihood, impact and risk ratings from drop downs. Risk matrix can be found in Appendix 1 (ALARP: As Low As Reasonably Practicable).

No.	Risk	Likelihood	Impact	Risk Rating	Mitigation
1	Collection: APS staff are identified as a result of privacy violation of Personal identifiable information.	Unlikely	Moderate	ALARP	Bespoke surveys collect data via surveys that will be voluntary to complete. Before each bespoke survey, SPRG will ensure all personal information collected complies with the APPs.
2	Collection: Personal information will be collected without a clear purpose, which could increase the risk of unauthorised uses and disclosures.	Unlikely	Minor	Acceptable	During bespoke survey questionnaire development stage, the content of the questionnaire is reviewed and where redundant / unused items exist, they are suggested for removal to the survey sponsor.
3	Notification of collection: Collection notice will not be provided to all individuals, for example those using non-standard communication channels	Unlikely	Minor	Acceptable	The collection notices for bespoke surveys are made accessible and embedded in the online survey.

No.	Risk	Likelihood	Impact	Risk Rating	Mitigation
4	Information security: The availability of the data is compromised as a result of a denial of service (DOS) attack.	Unlikely	Moderate	ALARP	**Microsoft Forms:** The Department of Finance has undertaken an IRAP assessment of GovTEAMS and accredited the system to hold information up to and including the OFFICIAL: Sensitive classification. Finance undertakes a risk-based approach to ICT Security, including Cloud Security. Finance follows Commonwealth Government Guidelines as laid out in the Information Security Manual https://acsc.gov.au/infosec/ism/ **Qualtrics:** Qualtrics' in-house Security Operations Center monitors the confidentiality, integrity, availability and performance of data with sophisticated intrusion detection systems, performance and health systems, and security event correlation systems. https://www.qualtrics.com/au/platform/security/?rid=ip&prevsite=en&newsite=au&geo=AU&geomatch=au
5	Information security: The confidentiality and integrity of the survey data is compromised as a result of a data breach (Malware hosting)	Unlikely	Major	ALARP	**Microsoft Forms:** Finance follows Commonwealth Government Guidelines as laid out in the Information Security Manual https://acsc.gov.au/infosec/ism/ **Qualtrics:** Qualtrics have a range of security measures in place to guard against data breaches. https://www.qualtrics.com/au/platform/security/?rid=ip&prevsite=en&newsite=au&geo=AU&geomatch=au
6	Disclosure: SPRG researcher publishes identifying personal information	Unlikely	Major	ALARP	SPRG researchers are trained in privacy protection and follow standard operating procedures. Data are published in aggregate form. Reports are cleared through Directors and Assistant Commissioner - SPRG.

6. Recommendations, Response, Review: Based on your compliance check and risk assessment, what still needs to be implemented?

- What changes to current practice are required?
- Which risk mitigation strategies should be introduced?
- Are there any agency-wide changes that need to be made?
- Should any further consultation be undertaken?
- Are privacy impacts so significant that the project should not proceed in its current form?
- How often will the PIA for this project be reviewed?

Recommendation	**Result (select from drop down)**	**Comment**
Review this PIA annually.	Accepted: Yet to be Implemented	
Craft a generic collection notice and ensure that it is linked to every bespoke survey.	Accepted: Already Implemented	
Project Manager (Name): Dr Nicole Steele	Date: 3 November 2020	X Dr Nicole Steele Director - Workforce Research and Analysis Signature:

Appendix 1: Risk Matrix

		Likelihood		
		Unlikely	Likely	Highly Likely
Impact	Minor	**Acceptable**	**ALARP***	**ALARP**
	Moderate	**ALARP**	**ALARP**	**ALARP**
	Major	**ALARP**	**ALARP**	**Unacceptable**

* ALARP: As Low As Reasonably Practicable