



Australian Government
The Treasury



Small Business Cyber Resilience Service

Privacy Impact Assessment – Agency Response

© Commonwealth of Australia 2024

This publication is available for your use under a [Creative Commons Attribution 4.0 International](https://creativecommons.org/licenses/by/4.0/legalcode) licence, with the exception of the Commonwealth Coat of Arms, the Treasury logo, photographs, images, third party materials, materials protected by a trademark, signatures and where otherwise stated. The full licence terms are available from creativecommons.org/licenses/by/4.0/legalcode.



Use of Treasury material under a [Creative Commons Attribution 4.0 International](https://creativecommons.org/licenses/by/4.0/legalcode) licence requires you to attribute the work (but not in any way that suggests that the Treasury endorses you or your use of the work).

Treasury material used ‘as supplied’

Provided you have not modified or transformed Treasury material in any way including, for example, by changing the Treasury text; calculating percentage changes; graphing or charting data; or deriving new statistics from published Treasury statistics – then Treasury prefers the following attribution:

Source: The Commonwealth of Australia.

Derivative material

If you have modified or transformed Treasury material, or derived new material from those of the Treasury in any way, then Treasury prefers the following attribution:

Based on Commonwealth of Australia data.

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are set out on the Department of the Prime Minister and Cabinet website (see www.pmc.gov.au/government/commonwealth-coat-arms).

Other uses

Enquiries regarding this licence and any other use of this document are welcome at:

Manager
Media Unit
The Treasury
Langton Crescent
Parkes ACT 2600
Email: media@treasury.gov.au

In the spirit of reconciliation, the Treasury acknowledges the Traditional Custodians of country throughout Australia and their connections to land, sea and community. We pay our respect to their Elders past and present and extend that respect to all Aboriginal and Torres Strait Islander peoples.

Contents

Contents	iii
Context.....	4
Recommendation 1.1 – Collection Notice	5
Recommendation 1.2 – Consent mechanisms.....	6
Recommendation 1.3 – Minimising collection of Client Information.....	7
Recommendation 2.1 – Documented arrangements with the Australian Signals Directorate (ASD)	8
Recommendation 2.2 – Reporting to ASD	9
Recommendation 3.1 – Technical protections	10
Recommendation 3.2 – Retention requirements	10

Context

The Department of the Treasury (the Treasury) has established the Small Business Cyber Resilience Service program (the Program).

The Program was announced as part of the *2023-2030 Australian Cyber Security Strategy*. Under Shield 1 of the Strategy, *Strong businesses and citizens*, the Program provides small businesses with free, tailored, person-to-person cyber security support.

The Program's two core functions are to:

- build the cyber resilience and capability of small businesses; and
- provide support to small businesses impacted by a cyber incident.

The Program is staffed by personnel who are, or will be, appropriately qualified, trained or experienced in cyber security, small business, and counselling clients in distress.

The Program is being delivered by a third-party provider, IDCARE (the Grantee). The Grantee is required to collect information from clients and disclose this information to the Australian Government for Program monitoring, assurance and evaluation purposes, as well as to provide visibility on the types and volumes of cyber threats facing the small business sector. The Grantee may also disclose information to other third-party support services as part of a referral process under the Program.

Treasury engaged Maddocks to conduct a Privacy Impact Assessment (PIA) of the information collection, disclosure and use requirements of the Program.

Treasury has implemented the PIA recommendations and provided the PIA to IDCARE to support its implementation of the recommended best-practice measures.

This document outlines the recommendations and Treasury's response.

Recommendation 1.1 – Collection Notice

We support Treasury working with the Grantee to develop a suitable Collection Notice for the Program. We recommend that the Grantee be instructed to ensure that all Client personnel who contact the Grantee are provided with a Collection Notice, in a form approved by Treasury. This should occur before the individual provides any personal information to the Grantee, or as soon as practicable afterwards.

The Collection Notice should contain the matters required by APP 5.2, including to describe how personal information will be collected, disclosed and used in the course of delivering the Program. It will be particularly important to reflect that:

- the Grantee may disclose information to other entities which may be able to offer additional support for Clients (in this PIA, called Referral Providers), including under programs and services delivered or coordinated by private sector entities such as IDCARE, and to government agencies such as the Australian Signals Directorate (ASD) and the Department of Home Affairs (Home Affairs), for the purposes of providing cyber security support and analysis;
- the Grantee may disclose information to other Australian Government agencies in connection with the Program, including to:
 - Treasury, which will use and disclose that information to manage and administer the Program, including to facilitate evaluation of the Program and for research and policy development purposes (which may include post-engagement surveys and/or data sharing with other government agencies such as the Australian Bureau of Statistics (ABS));
 - The Department of Industry, Science and Resources (Industry), which will use and disclose any personal information it receives in connection with the Program, to administer the funding arrangements for the Program; and
 - (depending on the outcomes following implementation of Recommendation 2.2 below) ASD, which will use and disclose information it receives in connection with the Program to undertake its cybersecurity functions and activities; and
- Treasury may use third party contractors to assist it with tasks in connection with the Program (such as evaluation), and may disclose personal information collected under the Program to those contractors for this purpose.

We suggest that it would be appropriate for a full Collection Notice to be made available on Grantee's and Treasury's website, with a truncated version (with a link to the full version) being displayed when a Client submits a Webform, or read or played if a Client telephones the Helpline.

Agency response: Support

The Grant Agreement includes a Privacy Attachment which outlines the privacy requirements the Grantee needs to comply with in delivering the services under the Program. The Privacy Attachment requires the Grantee to develop a suitable Collection Notice, in line with the specifications outlined in the recommendation.

Recommendation 1.2 – Consent mechanisms

We recommend that the Grantee be instructed to implement consent mechanisms to obtain consent from all Client personnel who contact the Grantee. The Grantee should be required to obtain consent:

- when the Grantee is first contacted – this consent should cover the handling of any personal information that is provided to the Grantee (and in particular, any sensitive information that they may provide such as about their racial or ethnic origin or any disability) in accordance with the Collection Notice. In addition, the Grantee should also:
 - explain to Client personnel that the Client’s participation in the Program is voluntary and their consent can be withdrawn at any time, by contacting the Grantee (and the Grantee should be contractually required to immediately notify Treasury of any such withdrawal, so that Treasury can ensure that no further use or disclosure is made of that personal information); and
 - be required to explain to Client personnel that they can only provide personal information about another individual (such as about a particular Client customer) to the Grantee, if that individual has given them express consent to do so;
- if the Grantee wishes to use their personal information for reporting individual case studies about the Program (although ideally the Grant Agreement would specify that the Grantee cannot include any personal information in its reporting of such case studies); and
- if the Grantee wishes to conduct a ‘warm handover’ of the Client to a Referral Provider.

Ideally, obtaining consent should involve the Client personnel taking an ‘active step’ to indicate their consent (such as by ticking a box in the Webform, or by verbally stating that they agree, with the Grantee required to keep a record in its Grantee’s case management system of the provision of this verbal consent).

Agency response: Support

The Privacy Attachment requires the Grantee to implement appropriate consent mechanisms, in line with the specifications outlined in the recommendation.

Recommendation 1.3 – Minimising collection of Client Information

We recommend that Treasury provide further clarity for the Grantee under the Grant Agreement about the types of personal information that should and should not be recorded in the Grantee's case management system. For example, the Grant Agreement (or any documents generated in accordance with the Grant Agreement) could specify that:

- the Grantee must only collect personal information if it is relevant to the delivery of services under the Program;
- the Grantee must not record any sensitive information about Client personnel, unless the individual has given their consent for the collection and subsequent use/disclosure of that information (see Recommendation 1.2); and
- the Grantee must not record any personal information about identified Client customers, or any other identified third-party individual, unless the Client personnel has expressly confirmed that the other individual has given their permission for their personal information to be disclosed to the Grantee, and handled in accordance with the Collection Notice.

We observe that provision of guidance that outlines the types of 'personal information' and 'sensitive information' that the Grantee is likely to encounter in delivering services under the Program, and how it can be handled, may enhance the likelihood of compliance with Treasury's requirements.

Agency response: Support

The Privacy Attachment requires the Grantee to minimise collection of client information, in line with the specifications outlined in the recommendation.

Recommendation 2.1 – Documented arrangements with the Australian Signals Directorate (ASD)

While ASD is not an APP entity for the purposes of the Privacy Act, we recommend that Treasury consider entering into documented arrangements with ASD (which could be in the form of a memorandum of understanding), which:

- set out the purpose(s) for which Treasury will disclose, and ASD will collect, Client Information as part of the Program (i.e. how ASD will use the Client Information it receives);
- specify the data items that will be provided to ASD (with the view to minimising the amount of any personal information to that which is clearly required by ASD);
- specify how ASD will receive those data items (i.e. directly from the Grantee, or via Treasury and/or Industry, depending on the outcomes of the implementation of Recommendation 2.2 below);
- if ASD will be provided any personal information, record that:
 - each individual to whom the personal information relates will have consented to the provision of their personal information to ASD, in accordance with consent requirements of the Privacy Act; and
 - Treasury is only sharing the minimum amount of personal information necessary for ASD to conduct its functions and activities; and
- clarify which entity will be the ‘data custodian’ of the Client Information once it is held by ASD, including for the purposes of the *Data Availability and Transparency Act 2022* (Cth).

Agency response: Support

Treasury has developed a document to record the data collection and data-sharing arrangements between Treasury, DISR, ASD and the Grantee. The document sits under the Grant Agreement and outlines the data items the Grantee is required to collect, the purpose for collecting each data item, the entities that each data item will be shared with, and the method for sharing this data, in line with the specifications outlined in the recommendation. The Grantee, DISR, Treasury and ASD have agreed to the document.

The *Data Availability and Transparency Act 2022* does not apply to the data-sharing arrangement for the Program.

Recommendation 2.2 – Reporting to ASD

We recommend that Treasury work with ASD to determine an appropriate cyber incident reporting arrangement for the Program, which balances the policy objectives that support ASD's need for the information, against the potential privacy impacts for Clients, their personnel and customers. This is likely to involve consideration of the data items that are required (and whether they need to include any personal information), and whether the Grantee should be required to:

- report details of all Client cyber incidents via the ReportCyber website (which is administered by ASD) within 24 hours;
- encourage Clients to themselves report cyber incidents via the ReportCyber website, with the Grantee being required to inform the Client if a mandatory cyber incident reporting requirement has been triggered; and/or
- collect the data required by the current Cyber Resilience Data Sheet and report this in near-real time directly to ASD, or through Industry and/or Treasury as an intermediary step.

If the Grantee will be required to collect data from Clients about cyber incidents, and that data needs to include personal information, we consider that the most privacy-enhancing option would be for the Grantee to be required to:

- only collect and report to ASD those data fields currently listed in the Cyber Resilience Data Sheet (with the Grantee required to encourage Clients to independently report further data about cyber incidents via ReportCyber) – this will minimise overcollection of Client Information by the Grantee and ASD, especially if volumetric, non-personal information is sufficient for the purposes of its cybersecurity activities and functions; and
- report that data directly to ASD (rather than via Treasury or Industry, which we understand have no other need to collect that information for their functions and activities).

Once the reporting arrangement has been agreed between Treasury and ASD, we also recommend that associated information flows be reflected in the Collection Notice for Clients (see Recommendation 1.1) and documented in the arrangements between Treasury and ASD (see Recommendation 2.1).

Agency response: Support

Treasury has worked with ASD to agree an appropriate cyber incident reporting arrangement. Under the arrangement, the Grantee will collect data from clients about any cyber incidents experienced and share this directly with ASD, as recommended. This arrangement minimises the amount of personal information that is shared with ASD.

Recommendation 3.1 – Technical protections

We recommend that, prior to the go-live date of the Program, Treasury satisfies itself as to the technical robustness of the Grantee's ICT systems (particularly, the case management system that will be used to handle and store Client Information), to ensure that the personal information in those systems will be sufficiently protected from misuse, interference and loss, and from unauthorised access, modification or disclosure. This recommendation could be implemented by including minimum security requirements for such systems in the Grant Agreement, and/or by Treasury conducting a cybersecurity review of those systems.

Agency response: Support

Under the Grant Agreement, the Grantee is required to maintain compliance with ISO 27001, an international standard for information security management systems. The Grantee must also demonstrate compliance on an annual basis.

Recommendation 3.2 – Retention requirements

We recommend that Treasury consider clarifying the Grantee's retention obligations in relation to personal information that it collects for the Program, to specify when the Grantee must deidentify or destroy that information (for example, upon termination or expiry of the Grant Agreement, or within 24 hours of a Client withdrawing their consent to participate in the Program). This could be achieved by including these specifications in the Grant Agreement, or in activity plans developed under the Grant Agreement.

Agency response: Support

The Privacy Attachment specifies the Grantee's information retention obligations, in line with the recommendation.