Australian Government
Department of Industry, Science and Resources
Department of the Treasury

Questions and Answers

Small Business Cyber Resilience Service Grant Opportunity

The Small Business Cyber Resilience Service (the Service) will fund one service provider up to $8.1 million to set up a free, tailored, person-to-person support that will help small businesses improve their cyber resilience and support small businesses impacted by a cyber incident.

Question	Response
What is the closing date and time for applications?	The closing date for the Small Business Cyber Resilience Service (SBCRS) Grant Opportunity is Friday 26 April 2024 at 5pm AEST.
Define "small business" for the purposes of the grant.	Please see the glossary in the Grant Opportunity Guidelines (the Guidelines). A small business is defined as a business with 19 or less full time (or equivalent) employees, including sole traders.
When the word "support" is mentioned, is this considered "guidance" or "technical support (like a helpdesk)"?	The Service is not to be considered a technical help desk, but more a support service to assist small businesses to improve cyber security (before an incident), and ability to recover from a cyber incident. However, a level of technical expertise is required to deliver the Service (*refer to section 5.1.1 of the Guidelines for service requirements*).
Do you have to be a small business to be eligible?	A business of any size is welcome to apply for the grant if it can provide the Service and meets the eligibility criteria (*refer to section 4 of the Guidelines for eligibility criteria*).

Question	Response
The grant is for a single company who will support small businesses throughout the country. Is there an opportunity for smaller Cyber Security Organizations to support their local community?	The Guidelines allow for joint applications. The opportunity for organisations to partner with others and submit a joint application exists. As only one grant will be approved, we will require a lead applicant for every joint application (*refer to section 7.2 of the Guidelines for further information regarding joint applications*).
When "engage technical personnel with experience" is stated, what experience is required, and will this be validated to ensure compliance?	Specific qualifications have not been included in the Guidelines, as there are a range of qualifications that will exist across cyber security, small business, and counselling clients in distress. It has been left open to the applicant to make the case for why its particular mix of skills are the most relevant, and why it has the right level of experience for the Service. The successful grantee will have to ensure it has the right mix of skills and/or experience and will be held to what has been nominated in the application. Personnel performing work in relation to the Service are to be appropriately qualified to perform the tasks indicated, and are to continue to maintain all relevant qualifications, licences, permits, approvals or skills for the duration of their involvement.
What are the expected service level requirements of the Service? Will the Service need to have specific operating hours and number of calls/enquiries processed?	The Guidelines state what is expected in terms of minimum service requirements *(section 5.1 and 5.1.1)* and eligible expenditure *(section 5.3*). It is important to remember the grant application is a proposal that outlines how the applicant intends to deliver the Service and achieve the desired outcomes of the grant program, throughout the project period. Considering the assessment criteria in the Guidelines (s*ection 6*), the application should include how the applicant proposes to ensure the Service is delivered successfully. Service level standards are not explicitly set out in the Guidelines, but what an applicant considers important, should be set out in the application. The applicant is asked to detail what it believes can be achieved (proposed

Question	Response
	targets) with the type of service it is proposing for this grant opportunity.
How is it proposed that customers that need help to build cyber resilience be supported, and does the customer journey need to be outlined in the application? Is it expected that a specific case management technology solution and associated architecture is proposed?	The application is a proposal that outlines how the applicant intends to deliver the Service and achieve the desired outcomes of the grant program, throughout the project period. Considering the assessment criteria in the Guidelines (s*ection 6*), the application should include how the applicant proposes to ensure the Service is delivered successfully.
Should any small business, regardless of industry, be able to receive an assessment?	Any small business, regardless of industry, should be able to receive the Service.
What are the program expectations for support to resolve social media related incidents?	The Guidelines state what is expected in terms of minimum service requirements *(section 5.1 and 5.1.1)* and eligible expenditure *(section 5.3*). It is expected that the applicant will propose how it would provide support to small businesses in this scenario. Keeping in mind that the Service should identify where the small business requires additional expertise to deal with their specific incident and facilitate a referral, as required. This would include identifying the relevant customer support services for key entities such as banks, telecommunications providers, and social media platforms among others (*refer to section 2 of the Guidelines for more information regarding what the Service should provide to deal with the immediate aftermath of an incident*).
What, if any, marketing initiatives might be undertaken to share the Service with small business owners?	Marketing has not been included as an eligible expenditure item for this grant. This does not prevent an applicant from conducting their own marketing or including a communication strategy in their application. The Department of the Treasury (Treasury) will be promoting the Service through dedicated activities (including advertising on cyber.gov.au, business.gov.au and promoted through the Minister's channels). As a government initiative, there will also be a certain level of directed traffic to the Service.

Question	Response
The grant guidelines outline that grantees are expected to "provide advice to small businesses drawing on the tailored plan produced as part of the health check (once available)". Can you explain more about the health check program, when it is expected to be incorporated into the Small Business Cyber Resilience Service, and what the health check plans are likely to look like?	The cyber security health check program will be an online interactive tool to enable small and medium businesses to self-assess their current cyber security maturity and receive guidance on strengthening their cyber security processes. The health check program will be delivered by the Department of Home Affairs. It is expected this service will be co-designed with industry in the coming months and will be finalised by the end of this year. The successful grantee will provide small businesses with advice and solutions on improving their cyber security which are aligned with existing guidance produced by the Australian Signals Directorate (ASD) and, when developed, the health check program.
Is travel across the country expected, or is this something that can be centralised in a Head Office environment?	We are not expecting travel will be required. However, travel is considered an eligible expenditure item. The Government will assess the appropriateness/necessity of travelling (or not) as part of an applicant's broader proposal and whether it achieves the Government's policy objectives and value for money considerations.
Are offshore contract resource costs eligible costs under the grant?	Offshore contract costs have not been listed as ineligible expenditure in the Guidelines. If an applicant is proposing to use offshore contract resources this should be outlined in the application. The Grantee is responsible for the performance of its obligations, including in relation to any tasks undertaken by subcontractors. However, it is also important to keep in mind that costs may be ineligible where it is decided that they do not directly support the achievement of the planned outcomes for the project or that they are contrary to the objective of the program. In this scenario, the applicant must ensure that adequate funds are available to meet the costs of any ineligible expenditure associated with the project (*refer to section 5.3 and 5.4 of the Guidelines for more information regarding eligible and ineligible expenditure*).

Question	Response
	We note the eligibility criteria requires the successful grant recipient to have an Australian Business Number (*refer to section 4 of the Guidelines for Eligibility criteria*).
How is it proposed that the Cyber Resilience Service will be positioned with other Federal Government Cyber services, as they appear to overlap in purpose?	The Government offers a range of different cyber security supports for individuals and businesses. This reflects the diversity of needs and varying levels of cyber security maturity within the Australian community, including the small business cohort. Supports targeting small businesses include Cyber Wardens program, the upcoming cyber security health check, and cyber.gov.au including the Cyber Security Hotline (1300CYBER1). The Small Business Cyber Resilience Service will work alongside these other supports and empower small businesses to manage their cyber security risks in a way that best suits their needs (*refer to section 2 of the Guidelines for more information about the program*). While the guidance provided through the Service will overlap with information that is available on cyber.gov.au, or through the cyber security health check for example, the Service's unique feature is that it will provide small businesses with an avenue for tailored, person-to-person support. In addition, the Service will also provide support in the aftermath of an attack, which is generally not a focus for other supports.
Is there any guidance in relation to the handover process between the Australian Signals Directorate (ASD) Cyber Hotline and the Service?	It is expected that the applicant will propose a solution on how referrals will be managed in the proposal, which forms part of the application. Please note, the Guidelines require that the Service will report near-real time raw data to ASD to provide visibility of types and volumes of threats facing the small business sector. Section 5.1.1 (Service requirements) of the Guidelines also requires that the successful grantee liaises with ASD to establish referral pathways and near real-time data sharing arrangements. The Treasury can help the

Question	Response
	successful grantee identify and make initial contacts.
How do we support technically challenged customers? If they are struggling with advice over the phone to make changes, is there a set view as to what a solution would look like in that scenario?	It is open to the applicant to propose what it thinks a solution would look like in this situation. These are the customers that need to be supported the most and targeted by the Service. Applicants will have to ensure that those operating the Service are able to talk to customers with low digital maturity.
The following is listed in the Guidelines as an item grant money can't be used for: 'Technical advice and support provided to a small business while they are experiencing a live cyber incident'. Why are costs related to this resourcing excluded? Is this not a critical, and expensive component in delivering the Service?	To be clear, the Guidelines do not exclude technical advice and support provided to a small business **before** or **after** a cyber incident from eligible expenditure. The Service is focussed on 'before' and 'after' a cyber incident. The Service has two core functions: • Building the cyber resilience and capability of small businesses **before** an incident • Providing support to small businesses impacted by a cyber incident **after** the incident Where the small business is **experiencing a live cyber incident**, the Service will need to refer the small business to the Cyber Security Hotline (1300CYBER1) for support. A small business that contacts cyber.gov.au to report an incident can be referred to the Service for assistance to recover from the incident. The cyber.gov.au website will also include contact details for the Service. In situations where the distinction between **live incident** and **after** an attack are unclear, general advice is that the Service can provide support if the client has made contact with cyber.gov.au or 1300CYBER1 to seek assistance.
In relation to skills in the call centre how will the Service be expected to capture forensic information for potential use in cyber-crime cases? Will training in evidence capture be expected? Would that be a requirement?	The applicant's proposal should explain how it would handle this situation if they think it is important.

Question	Response
Is the grant funding to be used to develop and launch the Service in 2026/27? Or is it expected that the Service will be delivered within the next three years?	Grant funding is to be used to deliver the Service over the next three years. The Government's expectation is that the Service will be able to aid small businesses this year. Specifics as to when the Service will be operational under your proposal should form a key part of your response to the assessment criteria (*refer to section 6 of the Guidelines for further information on the assessment criteria*).
As per the guidelines, funding is $8.1m over 3 years. With the successful tenderer having to evidentially show what they use grant funds for. What happens if all funding isn't used each year? Or the funding is exhausted early?	Funding will be fixed and capped each year consistent with section 3.1 of the Guidelines. Expenditure profiles will be discussed with the successful applicant, as part of the funding agreement negotiations. The expenditure of funds will be monitored throughout the grant period, and if there are deviations from the agreed funding profile, the Government will engage with the grantee on potential actions. Consideration on whether outcomes are being met as well as unmet demands for the Service will be central to these discussions.
How will success of the Service be measured over the duration of the grant?	The progress and success of the Service will be monitored in several different ways. There will be an agreed minimum data set which the successful grantee will be required to provide at regular intervals throughout the life of the grant agreement. This data will be used as part of the ongoing evaluation of the success of the Service (*refer to section 12 of the guidelines for information regarding how grant activity is monitored).* Additionally, the successful grantee will be required to monitor the quality and effectiveness of the service provided to small businesses, and the staff delivering them through surveys of clients' satisfaction and analysis of call data. The Treasury will also reach out periodically to clients that have accessed the Service, to gauge the quality and effectiveness of the service provided, and clients' satisfaction with them *(refer to section 5.1.1(3) of the guidelines for information regarding the data and reporting service requirements).*

Question	Response
Why only one provider to be appointed? I think it would be more efficient to appoint a 'panel' of providers that have specific skills or focus areas with cyber and/or incident response and management.	The Government will accept joint applications (*refer to section 7.2 of the Guidelines for more detail*) that can bring together different service providers as part of a consolidated service.
Is there an existing government aligned service looking after small business in a similar way or is this a new venture?	The Service is a new initiative by the Government.
Do you have a sense of the number of small businesses out there that would be impacted and require the Service?	Useful data sources that applicants may wish to consider include: The Australian Cyber Security Centre's 2022-23 Annual Cyber Threat Report for a view of the current cyber threat picture in Australia. The Australian Bureau of Statistics data on Australian Businesses for information on the number of small businesses in Australia.
Is it possible to provide support only in a remedial sense, after a small business has been scammed, to assist them to work out what happened? We are finding that they are often very confused and have trouble mapping out exactly what happened. After the mapping process is completed, it is easier for referral agencies to determine what has happened and how they can provide support.	This would potentially be considered eligible expenditure if such a mapping process was consistent with the mandatory requirements for this grant opportunity, as set out in section 5 of the Guidelines, under Eligible grant activities and Service requirements. The Guidelines require that the Service provides two core functions for small businesses: • Building the cyber resilience and capability of small businesses **before** an incident • Providing support to small businesses impacted by a cyber incident **after** the incident A mapping process **after** a cyber incident would only partially fulfill the requirements of the Service, which also needs to provide preventative support.
Are there any restrictions on the grantee doing additional commercial work for clients using the Cyber Resilience Service where their requirements exceed what can be provided under the Service?	The successful grantee is required to adhere to the conditions outlined in the grant agreement (which includes the Guidelines). Any activities falling outside of these parameters are not subject to the specified conditions but must not violate the program's service delivery obligations. Generally, there would be no restrictions in offering additional services to small business as long as Australian Privacy Principles are

Question	Response
	adhered to, the service offering is clearly identified as separate to the service. We would expect the successful recipient to be upfront about this arrangement, potentially including providing data about when this is occurring.
Can you explain the thinking behind setting the grant amount of $8.1m. Has this been built up from input assumptions, or is it simply the amount that has been allocated politically?	$8.1 million is the amount allocated by the Australian Government for the grant and applicants should detail the type of service that can be provided for this amount, consistent with the Guidelines.
Will the Service be delivered through the department as a vehicle? Or will the successful grantee be utilising their own ABN/business to represent the departments initiative?	The successful grantee will be utilising their own ABN/business whilst delivering the Service.
Will the provider be able to brand the Service or will it be given a generic name?	Applicants are welcome to include co-branding proposals in their application but should expect to use any branding alongside Small Business Cyber Resilience Service branding. Branding guidelines will be provided to the successful grantee.
What are the insurance requirements? Are there any limitations on the provider's liability?	The successful grantee will need to conduct an assessment to identify the risks associated with undertaking the Activity and maintain adequate and appropriate insurance to mitigate these risks. The Grantee will be required to provide proof of insurance to the Government upon request and within the time specified in the request. This is outlined in the sample grant agreement at section 16 of the Guidelines.
Do you have expectations that we verify the small businesses are legitimate and based in Australia before providing the Service?	Yes, we do expect the Service will verify the small business clients accessing the Service. It is up to the applicant to determine how this verification takes place. At a minimum Treasury expects the grantee to collect client ABNs. Any due diligence provisions need to be detailed and provided in the application.
Are foreign owned small businesses eligible to use the Service?	As per the Guidelines the program will fund one service provider to service small businesses **located across Australia**, in both metropolitan and regional locations.
Is there a transactional element to the grant (e.g., per call answered), or is it a fixed sum?	The grant is a fixed sum. The Government has announced a total of $8.1 million over 3 years from 2024-25 to 2026-27 for the program. The funding profile by year is: • $2.3 million in 2024-25 • $2.3 million in 2025-26

Question	Response
	• $3.5 million in 2026-27.
As this service will be provided as a "no-cost service" for small business, how will engagement be communicated to small business to ensure they understand what deliverables are included as part of the free service? Or is this to be communicated within the proposed plan?	The Government will be promoting the Service (including advertised on cyber.gov.au, business.gov.au, and promoted through the Minister's channels). As a government initiative, there will also be a certain level of directed traffic to the Service. The Treasury will work with the successful grantee on this messaging to ensure it aligns with the scope of the successful service offering. We would expect the applicant to set out how it would communicate the deliverables in its proposal.
Helping to protect small business will require recommending products. Are there any restrictions on what products or is it at the discretion of the grantee and their partners?	This would be a matter for the professional judgement of the successful grantee. However, such recommendations would need to be consistent with the objectives of the program.
The third-year funding profile has a significant increase from Year 1 and Year 2. Could it proposed to extend the program if operating costs remain at Year 1 and Year 2 costs?	No. The grant opportunity is bound by the program guidelines. This includes project period parameters.
Is there an expectation that the Service continues beyond the life of the grant?	The grant specifically covers the period up to 31 March 2027. The future of the Service beyond this period will be subject to normal government decision-making processes.