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

Grant Opportunity Guidelines

Small Business Cyber Wardens – ad hoc grant to the Council of Small Business Organisations of Australia Limited (ABN 43 008 597 304)

Commonwealth policy entity	The Treasury
Administering entity	Department of Industry, Science and Resources
Enquiries	If you have any questions, contact us on CyberWardens@industry.gov.au
Date guidelines released:	TBC
Type of grant opportunity	One off/ ad hoc

Contents

1. About the grant

Uplifting the capabilities of small businesses (defined as less than 20 employees, have an ABN and must be trading) will contribute to a strong baseline of cyber security for Australia, enabling all Australians to stay safe online and access the opportunities offered by the digital economy. The Small Business Cyber Wardens grant aims to empower small businesses to protect themselves against cyber threats, by supporting them to build their in-house capability to do so. The grant contributes to Treasury's Outcome 1.3: Support for Markets and Business.

The objective of the grant is to build the capabilities of small businesses to protect themselves from cyber security threats.

The intended outcomes of the grant are:

- a greater awareness amongst small business nationally of cyber security threats
- small businesses take action to protect themselves from cyber security threats
- small businesses have trained in-house cyber wardens to guard against cyber security threats.

We administer the program according to the *Commonwealth Grants Rules and Guidelines* (CGRGs)[1].

2. Grant amount and grant period

The Australian Government has announced up to $22.995 million over three years from 2023-24 to 2025-26.

3. Grant selection process

This grant opportunity is a one-off or ad hoc grant. The Treasury considers that this is an appropriate type of selection process considering the nature of the grant is specifically dependent on the Council of Small Business Organisations of Australia Limited (COSBOA) because:

- it is Australia's peak body representing the interests of small businesses and has extensive experience in working with this very diverse group
- it is trusted by small business to promote and support the development of small businesses in Australia and is a credible advocate for advancing their interests
- it has a strong history of fostering an increased awareness and understanding of the role of small business in the general community
- it can directly reach a vast range of small businesses and has strong links through their membership body into many local communities
- it conceived, designed and developed the cyber wardens concept.

3.1. Eligibility criteria

The grantee is the Council of Small Business Organisations of Australia Limited, ABN 43 008 597 304.

3.2. Who is not eligible?

You are not eligible to apply if:

[1] https://www.finance.gov.au/government/commonwealth-grants/commonwealth-grants-rules-guidelines

- you or your project partner is listed on the National Redress Scheme's website as an institution that has not joined or signified its intent to join the Scheme (www.nationalredress.gov.au)
- you have 100 or more employees and have not complied with the *Workplace Gender Equality Act (2012)*.

3.3. Eligible activities

To be eligible your project must:

- be aimed at uplifting the cyber security awareness and capability of small businesses.

Eligible activities may include:

- research, consultation and reporting on small business cybersecurity perceptions, needs and impact, and industry co-design
- program and platform development including design and ongoing delivery of the eLearning program and platform
- communication including campaigns and/or media including national events and research whitepapers
- development of industry stakeholder resources
- awareness-building and education including a national awareness communication strategy, including media and stakeholder engagement
- recruitment and participant support
- project management and evaluation.

We may also approve other activities.

3.4. Eligible expenditure

You can only spend grant funds on eligible expenditure you have incurred on an agreed project as defined in your grant agreement.

Eligible expenditure items include:

- direct labour costs of employees you directly employ on the core elements of the project. We consider a person an employee when you pay a regular salary or wage, out of which you make regular tax instalment deductions
- up to 30 per cent labour on costs to cover employer paid superannuation, payroll tax, workers compensation insurance, and overheads such as office rent and the purchase or provision of computing equipment directly required or related to the delivery of the project
- contract expenditure covering the cost of eligible project activities that are contracted to others. All contractors must have a written contract prior to starting any project work. Invoices from contractors must contain a detailed description and breakdown of the work including hours and hourly rates
- domestic travel limited to the reasonable cost of accommodation and transportation required to conduct agreed project activities in Australia
- staff training that directly supports the achievement of project outcomes
- ICT costs directly relevant to the project
- costs associated with media campaigns, including promotional material, directly related to the project

- the cost of an independent audit of project expenditure (where we request one) up to a maximum of 1 per cent of total eligible project expenditure
- contingency costs up to a maximum of 10 per cent of the eligible project costs. Note that we make payments based on actual costs incurred.

If your application is successful, we may ask you to verify project costs that you provided in your application. You may need to provide evidence such as quotes for major costs.

Not all expenditure on your project may be eligible for grant funding. The program delegate (who is a general manager within the department with responsibility for administering the program) makes the final decision on what is eligible expenditure and may approve other activities.

To be eligible, expenditure must:

- be a direct cost of the project, or
- be incurred by you for required project audit activities.

You must incur the project expenditure between the project start and end date for it to be eligible unless stated otherwise. You must not commence your project until your grant agreement is executed. We are not responsible for any expenditure you incur until a grant agreement is executed. The Commonwealth will not be liable, and should not be held out as being liable, for any activities undertaken before the grant agreement is executed.

3.5. Ineligible expenditure

Expenditure of ineligible expenditure include:

- research not directly supporting eligible activities
- activities, equipment or supplies that are already being supported through other sources
- costs incurred prior to the grant agreement being executed
- any in-kind contributions
- financing costs, including interest
- capital expenditure for the purchase of assets such as office furniture and equipment, motor vehicles, computers, printers or photocopiers and the construction, renovation or extension of facilities such as buildings and laboratories
- costs such as rental, renovations and utilities
- non-project-related staff training and development costs
- costs related to obtaining resources used on the project, including interest on loans, job advertising and recruiting, and contract negotiations
- depreciation of plant and equipment beyond the life of the project
- maintenance costs.

This list is not exhaustive and applies only to the expenditure of the grant funds. Other costs may be ineligible where we decide 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.

You must ensure you have adequate funds to meet the costs of any ineligible expenditure associated with the project.

4. Your proposal

The grant is subject to an acceptable proposal that includes:

- contact name and position details
- project description
- project start and end date
- details of project milestones including the key activities relevant to each milestone
- details of project governance
- a risk management plan
- details of project partners and collaborators
- detailed project budget (split over financial years and by activity), including justification of major cost elements.

5. How to submit your proposal

You will need to set up an account to access our online portal. The portal allows you to apply for and manage a grant or service in a secure online environment. To submit your proposal, you must:

- complete an application through the portal
- provide all the information requested
- address all eligibility criteria
- include all necessary attachments.

You can view and print a copy of your submitted application on the portal for your own records.

You are responsible for making sure your application is complete and accurate. Giving false or misleading information is a serious offence under the *Criminal Code Act 1995* (Cth). If we consider that you have provided false or misleading information we may not progress your application. If you find an error in your application after submitting it, you should call us immediately on 13 28 46.

If we find an error or information that is missing, we may ask for clarification or additional information from you that will not change the nature of your application.

If you need further guidance around the application process, or if you have any issues with the portal, contact us at business.gov.au or by calling 13 28 46.

6. How we assess your proposal

In assessing your proposal, we will consider whether:

- your project aligns with the policy intent
- your project is appropriately costed and represents value with relevant money
- your proposed activities and expenditure are eligible
- the level of risk associated with the project and its implementation is manageable and acceptable
- you can deliver your project on time and to budget as identified in supporting documents.

7. Who will approve the grant?

The program delegate will make the final decision to approve the grant.

The program delegate's decision is final in all matters, including:

- the grant approval
- the grant funding to be awarded
- any conditions attached to the offer of grant funding.

The program delegate must not approve grant funding if they reasonably consider the program funding across financial years will not accommodate the grant funding offer or if the application does not represent value for relevant money.

8. Notification of the grant

We will advise you of the outcome of your application in an email. If you are successful, we advise you of any specific conditions attached to the grant.

9. Grant agreement

You must enter into a legally binding grant agreement with the Commonwealth. The grant agreement has general terms and conditions that cannot be changed.

We will manage the grant agreement through the portal. Accepting the agreement through the portal is the equivalent of signing a grant agreement. After you have accepted it we will execute the agreement. Execute means both you and the Commonwealth Government have entered into the grant agreement. We will notify you when a copy of the executed agreement is available through the portal. The agreement will not become binding until it is executed.

We must execute a grant agreement with you before we can make any payments. We are not responsible for any expenditure you incur before a grant agreement is executed.

Upon execution of the agreement, you agree you will obtain written informed consent from activity participants to share their information in accordance with the Australian Privacy Principles (APPs) and the *Privacy Act 1988* (Cth) for the purpose of assurance and evaluation activities.

The approval of your grant may have specific conditions determined by the assessment process or other considerations made by the program delegate. We will identify these in the offer of grant funding.

If you enter an agreement under this grant opportunity, you cannot receive other grants for this project from other Commonwealth, state or territory granting programs.

The Commonwealth may recover grant funds if there is a breach of the grant agreement.

You will have 30 days from the date we notify you of your success to execute the grant agreement with the Commonwealth. During this time, we will work with you to finalise details.

The offer may lapse if both parties do not accept the grant agreement within this time. Under certain circumstances, we may extend this period. We base the approval of your grant on the information you provide in your application. We will review any required changes to these details to ensure they do not affect the project as approved by the program delegate.

9.1. Variations to the grant agreement

We recognise that unexpected events may affect project progress. In these circumstances, you can request a variation to your grant agreement, including:

- changing project milestones
- changing project activities

- extending the timeframe for completing the project.

If you want to propose changes to the grant agreement, you must put them in writing before the project end date, for the program delegate to consider.

9.2. Project specific legislation, policies and industry standards

You must comply with all relevant laws, regulations and Australian Government sanctions in undertaking your project. You must also comply with the specific legislation/policies/industry standards that follow. It is a condition of the grant funding that you meet these requirements. We will include these requirements in your grant agreement.

In particular, you will be required to comply with State or territory legislation in relation to working with children.

9.3. Tax obligations

If you are registered for the Goods and Services Tax (GST), where applicable we will add GST to your grant payment and provide you with a recipient created tax invoice. You are required to notify us if your GST registration status changes during the project period. GST does not apply to grant payments to government related entities[2].

Grants are assessable income for taxation purposes, unless exempted by a taxation law. We recommend you seek independent professional advice on your taxation obligations or seek assistance from the Australian Taxation Office[3]. We do not provide advice on tax.

10. Grant acquittal, payment and reporting

10.1. How we pay the grant

We will make payments according to an agreed schedule set out in the grant agreement. Payments are subject to satisfactory progress on the project.

10.2. Keeping us informed

You should let us know if anything is likely to affect your project or organisation.

We need to know of any key changes to your organisation or its business activities, particularly if they affect your ability to complete your project, carry on business and pay debts due.

You must also inform us of any changes to your:

- name
- addresses
- nominated contact details
- bank account details.

If you become aware of a breach of terms and conditions under the grant agreement, you must contact us immediately.

You must notify us of events relating to your project and provide an opportunity for the Minister or their representative to attend.

[2] See Australian Taxation Office ruling GSTR 2012/2 available at ato.gov.au

[3] https://www.ato.gov.au/

10.3. Reporting

You must submit reports through the portal in line with the grant agreement. We will provide the requirements for these reports as appendices in the grant agreement. We will remind you of your reporting obligations before a report is due. We will expect you to report on:

- progress against agreed project milestones
- project expenditure, including expenditure of grant funds.

The amount of detail you provide in your reports should be relative to the project size, complexity and grant amount.

10.3.1. Progress reports

Progress reports must:

- include details of your progress towards completion of agreed project activities
- show the total eligible expenditure incurred to date
- include evidence of expenditure
- be submitted by the report due date (you can submit reports ahead of time if you have completed relevant project activities)
- include data on the small businesses engaged and individuals enrolled, certified and re-certified through your program each quarter
- data on research, awareness and education campaigns conducted throughout the quarter.

We will only make grant payments when we receive satisfactory progress reports.

You must discuss any project or milestone reporting delays with us as soon as you become aware of them.

10.3.2. End of project report

When you complete the project, you must submit an end of project report.

End of project reports must:

- include the agreed evidence as specified in the grant agreement
- identify the total eligible expenditure incurred for the project
- include a declaration that the grant money was spent in accordance with the grant agreement and to report on any underspends of the grant money
- be submitted by the report due date
- include data on the small businesses engaged and individuals enrolled, certified and re-certified through your program
- data on research, awareness and education campaigns conducted throughout the project.

10.3.3. Ad-hoc reports

We may ask you for ad-hoc reports on your project. This may be to provide an update on progress, or any significant delays or difficulties in completing the project.

10.4. Independent audits

We will ask you to provide an independent audit report. An audit report will verify that you spent the grant in accordance with the grant agreement. The audit report requires you to prepare a statement

of grant income and expenditure. The report template is available on business.gov.au and GrantConnect.

10.5. Compliance visits

We may visit you during the project period to review your compliance with the grant agreement. We may also inspect the records you are required to keep under the grant agreement. We will provide you with reasonable notice of any compliance visit.

11. Grant acknowledgement

If you make a public statement about a project funded under the program, including in media releases, on social media and in a brochure or publication, you must acknowledge the grant by using the following:

'This project received grant funding from the Australian Government.'

12. Announcement of grants

We publish details of successful projects on GrantConnect as required by the *Commonwealth Grants Rules and Guidelines* unless otherwise prohibited by law. We may also publish this information on business.gov.au. This information may include:

- name of your organisation
- title of the project
- description of the project and its intended outcomes
- amount of grant funding awarded
- Australian Business Number
- business location
- your organisation's industry sector.

13. Probity

We will make sure that the grant opportunity process is fair, according to the guidelines, incorporates appropriate safeguards against fraud, unlawful activities and other inappropriate conduct and is consistent with the CGRGs.

13.1. Conflicts of interest

Any conflicts of interest could affect the performance of the grant opportunity or program. There may be a conflict of interest, or perceived conflict of interest, if our staff, or our Commonwealth Policy entity staff, any member of a committee or advisor and/or you or any of your personnel:

- has a professional, commercial or personal relationship with a party who is able to influence the application selection process, such as an Australian Government officer
- has a relationship with or interest in, an organisation, which is likely to interfere with or restrict the applicants from carrying out the proposed activities fairly and independently or
- has a relationship with, or interest in, an organisation from which they will receive personal gain because the organisation receives a grant under the grant program/ grant opportunity.

As part of your application, we will ask you to declare any perceived or existing conflicts of interests or confirm that, to the best of your knowledge, there is no conflict of interest.

If you later identify an actual, apparent, or perceived conflict of interest, you must inform us in writing immediately.

Conflicts of interest for Australian Government staff are handled as set out in the Australian Public Service Code of Conduct (Section 13(7))[4] of the *Public Service Act 1999* (Cth). Committee members and other officials including the decision maker must also declare any conflicts of interest.

We publish our conflict of interest policy[5] on the department's website. The Commonwealth policy entity also publishes a conflict of interest policy on its website.

13.2. How we use your information

Unless the information you provide to us is:

- confidential information as per 13.2.2, or
- personal information as per 13.2.3,

we may share the information with other government agencies for a relevant Commonwealth purpose such as:

- to improve the effective administration, monitoring and evaluation of Australian Government programs
- for research
- to announce the awarding of grants.

13.2.1. How we handle your confidential information

We will treat the information you give us as sensitive and therefore confidential if it meets all of the following conditions:

- you clearly identify the information as confidential and explain why we should treat it as confidential
- the information is commercially sensitive
- disclosing the information would cause unreasonable harm to you or someone else
- you provide the information with an understanding that it will stay confidential.

13.2.2. When we may disclose confidential information

We may disclose confidential information:

- to our Commonwealth employees and contractors, to help us manage the program effectively
- to the Auditor-General, Ombudsman or Privacy Commissioner
- to the responsible Minister or Assistant Minister
- to a House or a Committee of the Australian Parliament.

We may also disclose confidential information if

- we are required or authorised by law to disclose it
- you agree to the information being disclosed, or

[4] https://www.legislation.gov.au/Details/C2019C00057

[5] https://www.industry.gov.au/publications/conflict-interest-policy

- someone other than us has made the confidential information public.

13.2.3. How we use your personal information

We must treat your personal information according to the Australian Privacy Principles (APPs) and the *Privacy Act 1988* (Cth). This includes letting you know:

- what personal information we collect
- why we collect your personal information
- to whom we give your personal information.

We may give the personal information we collect from you to our employees and contractors, and other Commonwealth employees and contractors, so we can:

- manage the program
- research, assess, monitor and analyse our programs and activities.

We, or the Minister, may:

- announce the names of successful applicants to the public
- publish personal information on the department's websites.

You may read our Privacy Policy[6] on the department's website for more information on:

- what is personal information
- how we collect, use, disclose and store your personal information
- how you can access and correct your personal information.

13.2.4. Freedom of information

All documents in the possession of the Australian Government, including those about the program, are subject to the *Freedom of Information Act 1982* (Cth) (FOI Act).

The purpose of the FOI Act is to give members of the public rights of access to information held by the Australian Government and its entities. Under the FOI Act, members of the public can seek access to documents held by the Australian Government. This right of access is limited only by the exceptions and exemptions necessary to protect essential public interests and private and business affairs of persons in respect of whom the information relates.

If someone requests a document under the FOI Act, we will release it (though we may need to consult with you and/or other parties first) unless it meets one of the exemptions set out in the FOI Act.

13.3. Enquiries and feedback

For further information or clarification, you can contact us on 13 28 46 or by web chat or through our online enquiry form on business.gov.au.

We may publish answers to your questions on our website as Frequently Asked Questions.

Our Customer Service Charter is available at business.gov.au. We use customer satisfaction surveys to improve our business operations and service.

If you have a complaint, call us on 13 28 46. We will refer your complaint to the appropriate manager.

[6] https://www.industry.gov.au/data-and-publications/privacy-policy

If you are not satisfied with the way we handle your complaint, you can contact:

General Manager
Business Grants Hub

Department of Industry, Science and Resources

GPO Box 2013
CANBERRA ACT 2601

You can also contact the Commonwealth Ombudsman[7] with your complaint (call 1300 362 072). There is no fee for making a complaint, and the Ombudsman may conduct an independent investigation.

[7] http://www.ombudsman.gov.au/

Commonwealth Standard Grant Agreement

between the Commonwealth of Australia represented by

Department of Industry, Science and Resources

and

COUNCIL OF SMALL BUSINESS ORGANISATIONS OF AUSTRALIA LIMITED

The Commonwealth Acknowledges the Aboriginal and Torres Strait Islander Peoples throughout Australia and their continuing connection to land, water, culture and community. We pay our respects to the Elders both past and present. We acknowledge that our services are provided on many Indigenous lands. We continue to recognise that to achieve true reconciliation we need to work together with Aboriginal and Torres Strait Islander peoples, communities, staff and stakeholders to ensure that we are meeting the needs of the community.

Contents

Grant Agreement SBCW000001

Once completed, this document, together with the Grant Details and the Commonwealth Standard Grant Conditions (Schedule 1), forms an Agreement between the Commonwealth of Australia (the Commonwealth) and the Grantee.

Parties to this Agreement

The Grantee

Full legal name of Grantee	COUNCIL OF SMALL BUSINESS ORGANISATIONS OF AUSTRALIA LIMITED
Legal entity type (e.g. individual, incorporated association, company, partnership, etc)	Australian Public Company
Trading or business name	COUNCIL OF SMALL BUSINESS ORGANISATIONS OF AUSTRALIA LTD
Any relevant licence, registration or provider number	Not applicable
Australian Business Number (ABN) or other entity identifiers	43008597304
Australian Company Number (ACN)	008597304
Registered for Goods and Services Tax (GST)?	Yes
Date from which GST registration was effective?	24/07/2000
Registered office address	15 MOORE ST CANBERRA ACT 2601 Australia
Relevant business place	ANZ Building, Level 2 15 Moore Street Canberra ACT 2601 Australia

The Commonwealth

The Commonwealth of Australia represented by the
Department of Industry, Science and Resources
of 10 Binara Street CANBERRA ACT 2600
ABN 74 599 608 295

The Department of Industry, Science and Resources will manage the Agreement on behalf of the Treasury.

Background

The Commonwealth has agreed to enter this Agreement under which the Commonwealth will provide the Grantee with a Grant for the purpose of assisting the Grantee to undertake the associated Activity.

The Grantee agrees to use the Grant and undertake the Activity in accordance with this Agreement and the relevant Grant Details.

Scope of this Agreement

This Agreement comprises:

(a) this document;

(b) the Supplementary Terms (if any);

(c) the Standard Grant Conditions (Schedule 1);

(d) the Grant Details;

(e) any other document referenced or incorporated in the Grant Details.

If there is any ambiguity or inconsistency between the documents comprising this Agreement in relation to a Grant, the document appearing higher in the list will have precedence to the extent of the ambiguity or inconsistency.

This Agreement represents the Parties' entire agreement in relation to the Grant provided under it and the relevant Activity and supersedes all prior representations, communications, agreements, statements and understandings, whether oral or in writing.

Certain information contained in or provided under this Agreement may be used for public reporting purposes.

Grant Details SBCW000001

A. Purpose of the Grant

The Grant is being provided as part of the Small Business Cyber Wardens grant opportunity.

The objective of the grant is to build the capabilities of small businesses to protect themselves from cyber security threats.

The intended outcomes of the grant are:
• a greater awareness amongst small business nationally of cyber security threats
• small businesses take action to protect themselves from cyber security threats
• small businesses have trained in-house cyber wardens to guard against cyber security threats.

B. Activity

The Activity is made up of the Grantee's project and all eligible project activities as specified in these Grant Details.

Project title

Cyber Wardens

Project scope and description

The program's final milestones, deliverables, and budget will be agreed between COSBOA and the Department in an updated Project Plan provided in Milestone 1 to ensure alignment with the government's Cyber Strategy.

Full details of program activities, including breakdown of program deliverables, are included in the attached Project Plan.

Indicative activities:
Workstream #1: Research and evidence
#1.1 Annual 'Small Business Cyber Security Pulse Check' report
Research whitepaper providing 'state of the nation's small business and cyber security benchmarking, with a focus on measuring behavioural change and tracking emerging needs of Australian small business owners.
#1.2 National small business cyber security survey on preparedness and capability of small business owners and teams. Survey to be repeated annually over the life of the grant.
#1.3 Qualitative research
Focus groups and in-depth interviews across a range of small business sizes and demographic segments (including sole traders, micro SBs, mid-sized SBs, rural businesses, as well as founders who identify as female, culturally and linguistically diverse, Aboriginal and Torres Strait Islander and founders with a disability.)
#1.4 Communication and distribution strategy inclusive of annual industry research briefings and webinar, national media research launch and associated media support.

Workstream #2: Industry consultation and co-design
#2.1 General program consultation
Consultation and codesign activities to inform national Cyber Wardens program development. Building on Level 1, developed through the pilot program, Cyber Wardens Levels 2 and 3 will be

implemented in Year 1, with 3x Industry / Sector specific extensions in Year 2.
#2.2 Program Translation Consultation
Co-design and consultation with diverse audience segments.
#2.3 Program Expansion Report
Co-design and consultation recommendations and report synthesising insights and recommendations from codesign activities.
#2.4 Small Business Cyber Security 5 Year Strategy
Design of 5 Year Small Business Cyber Security Strategy with Cyber Wardens program recommendations.

Workstream #3: Program & platform development
#3.1 Educational design
Design of the educational outcomes and learning framework to guide the development of individual course components.
#3.2 E-learning modules and content development
End-to-end content and module development for the Cyber Wardens platform comprising wireframes, content creation, user testing and ongoing content maintenance
#3.3 Facilitated learning development
Development of content resources to support in-person learning, immersion workshops and facilitated sessions.
#3.4 Small business Cyber Wardens Resources Hub
Practical small business resources
#3.5 Brand
Cyber Wardens brand review and refinement.
#3.6 Platform hosting and management
Technical development, platform upgrades, maintenance, hosting, management.
#3.7 Cyber security
Security stress-testing of platforms and insurance

Workstream #4: National awareness and education campaign
#4.1 National awareness and education campaign
33-month awareness and education plan, with annual review and update to identify emerging opportunities and integrate them into the communication strategy.
#4.2 Media
National and industry media events and PR, alongside ongoing social media
#4.3 Stakeholder engagement
Ongoing engagement with small business peak body organisations
#4.4 Awareness content and activities
Ambassadors program, Cyber Wardens Local Training Stations, Local Electorate Cyber Wardens Kits, podcast, and major video campaign.
#4.5 Paid amplification
Paid advertising and media.

Workstream #5: Student recruitment and behavioural change
#5.1 Recruitment
Targeted and tailored recruitment activities for new learners, recertification and future modules
#5.2 Student support
Design and delivery of communications to students
#5.3 Graduation
Development, manufacture and fulfilment of graduation kit and recertification materials

#5.4 Driving behavioural change
Implementation program

Workstream #6: Reporting and evaluation
#6.1 Project Reporting
Grant reporting
#6.2 Evaluation
Design of student evaluation framework, survey creation and testing, market research approvals, collection and reporting

Workstream #7: Project management
#7.1 Work plan
Design of the 3-year program implementation work plan
#7.2 Advisory Group Management
Quarterly meetings of the Cyber Wardens Industry Advisory Group
#7.3 Project & Grant Management
Including financial and operations oversight of project sourcing, management of contractors, and so on

Project outcomes

A 3-year investment from the Australian Government would deliver Australia's first small business cyber security frontline comprised of employees and owners from the nation's 2.3 million small businesses. This investment would supercharge behavioural change in homes and businesses across Australia - with safer online practices closing Australia to the business of cyber criminals.

Rolling out the Cyber Wardens program nationally will:
1. Empower small businesses to help protect themselves against cyber threats by training up to 60,000 Cyber Wardens across at least 15,000 small businesses with free access to the Cyber Wardens eLearning program.

2. Increase small business awareness of cyber security threats and awareness of readily available solutions to build their cyber resilience by engaging with more than 1 million small business owners and employees through a high-impact national awareness campaign.

3. Build a network of trained in-house cyber wardens to drive cultural change and cyber-safe mindsets in Australia's small business.

4. Develop the practical skills of small businesses to guard against cyber security threats.

5. Provide a platform for small business to respond quickly to emerging cyber threats with targeted information and resources.

6. National program footprint including 24 Cyber Wardens roadshow events and the supply of local Cyber Wardens kits.

Nearly half of all Australians employed in small businesses have experienced a negative cyber incident. If just 20 per cent of businesses trained by Cyber Wardens could successfully detect and thwart a cyberattack, the financial gain for the industry could amount to $117 million. This equates to a potential ROI of at least 4x.

In undertaking the Activity, the Grantee must comply with the requirements of the grant opportunity guidelines (as in force at the time of application).

The Grantee must notify the Commonwealth about events relating to the project and provide an opportunity for the Minister or their representative to attend.

C. Duration of the Grant

The Activity starts on 06 November 2023 and ends on 31 July 2026, which is the **Activity Completion Date**.

The Agreement ends on 07 January 2027 which is the **Agreement End Date**.

Activity Schedule

In undertaking the Activity, the Grantee will meet the following milestones by the due dates.

Milestone number	Milestone name and description	Due date
001	Milestone 1: Project Launch & Design Project Plan with detailed milestones and deliverables confirmed. Risk Register and Mitigation Plan design Program Launch Evaluation design Inaugural Small Business Cyber Security Research Project and associated media and research webinar Program Learning Framework and strategy design Pilot content review Launch ambassador program Student recruitment, graduation and support services Project Management Resource Hub launch Content production National awareness & education campaign Measurable Targets: - Quantified outputs are described and/or achieved as outlined in the project plan for milestone 1 - Enrolments 1,000 - Graduates 500 - Small businesses engaged 150 The grantee is required to supply additional budget evidence in their first progress report as follows: - The grantee supplies further evidence to labour costs by specifying the funded positions inclusive of Part-Time/Full-Time Equivalent (PTE/FTE) staffing and the number of staff associated with direct labour costs. - The grantee supplies further evidence to travel expenditure such as class of travel, duration, accommodation, and number of travellers.	29/02/2024

Milestone number	Milestone name and description	Due date
002	Milestone 2: Facilitated Learning Design & Consultation Local Activations Kit and Local Electorate Pop-Ups Program Extension Consultation across program levels, audience translations and industries. Annual Recertification strategy, wireframes, content creation, user testing and platform development Program Extension: Emerging threat module development (if required). Train the Advisor & facilitate learning strategy, content and resource development. Podcast development and launch Student recruitment, graduation and support services Project Management Resource Hub management Content production National awareness & education campaign Measurable Targets: - Quantified outputs are described and/or achieved as outlined in the project plan for milestone 2 - Enrolments 6,500 - Graduates 5,500 - Small businesses engaged 1,650	31/07/2024
003	Milestone 3: Program Extension Recertification platform production Level 2 & 3 design and content production Train the Advisor final production and launch Program extensions: Emerging Threat module development and Lunch & Learn Kits Program adaptations: CALD translations and target audience-tailored content Annual Small Business Cyber Security Research Project and associated media Student recruitment, graduation and support services Project management Resource Hub management Content production National awareness & education campaign Measurable Targets: - Quantified outputs are described and/or achieved as outlined in the project plan for milestone 3 - Enrolments 9,500 - Graduates 8,300 - Recertification 1,500 - Small businesses engaged 2,490	31/01/2025

Milestone number	Milestone name and description	Due date
004	Milestone 4: Mid project impact and program amplification Mid-project impact report Level 2 & 3 Launch Program Extension: Emerging threat module user testing & sector extension development Program adaptations: Final production for train the advisor, CALD & Aboriginal and Torres Strait Islander targeted content Development and launch of podcast season 2 Student recruitment, graduation and support services Project management Resource Hub management Content production National Awareness & education campaign Measurable Targets: - Quantified outputs are described and/or achieved as outlined in the project plan for milestone 4 - Enrolments 12,000 - Graduates 10,700 - Recertification 4,500 - Small businesses engaged 3,210	31/07/2025
005	Milestone 5: Program amplification Ongoing project delivery Program Adaptations: CALD translations Annual Small Business Cyber Security Research Project and associated media Program Extension: Emerging threat module Annual Content Review Student recruitment, graduation and support services Project management Resource Hub management Content production National Awareness & education campaign Measurable Targets: - Quantified outputs are described and/or achieved as outlined in the project plan for milestone 5 - Enrolments 16,000 - Graduates 13,000 - Recertification 7,500 - Small businesses engaged 3,900	31/01/2026

Milestone number	Milestone name and description	Due date
006	Milestone 6: Amplification + evaluation Ongoing project delivery Project Evaluation National Awareness & education campaign inclusive off media + trade media campaign, 3 webinars, 3 trade booth, quarterly ambassador, branded content partnership Paid amplification 250K + 1250K search Project Management Resource Hub management Content production National Awareness & education campaign Measurable Targets: - Quantified outputs are described and/or achieved as outlined in the project plan for milestone 6 - Enrolments 15,000 - Graduates 12,000 - Recertification 10,500 - Small businesses engaged 3,600	31/07/2026

D. Payment of the Grant

The total amount of the Grant is $22,994,750 (plus GST if applicable).

The Grant will be provided at up to 100.00 per cent of eligible expenditure as defined in the grant opportunity guidelines subject to availability of Program funds.

The Grant will be paid in accordance with clause ST2.

The Grant will be paid according to the following schedule. Payments are subject to satisfactory progress on the project and compliance by the Grantee with its obligations under this Agreement.

Payment event	Payment amount (GST excl)	Anticipated payment date
Initial payment upon execution of this Agreement	s 47(1)(b)	21/11/2023
Progress payment		14/03/2024
Progress payment		30/09/2024
Progress payment		31/03/2025
Progress payment		30/09/2025
Final payment		31/03/2026
Total	$22,994,750	

Invoicing

The Grantee agrees to allow the Commonwealth to issue it with a Recipient Created Tax Invoice (RCTI) for any taxable supplies it makes in relation to the Activity.

E. Reporting

The Grantee agrees to provide the following reports to the Commonwealth representative in accordance with the reporting requirements (Schedule 2).

Report type	Period start date	Period end date	Agreed evidence	Due date
Progress Report 1	06/11/2023	31/01/2024	Detailed contract expenditure, Service level data	15/02/2024
Progress Report 2	01/02/2024	30/04/2024	Detailed contract expenditure, Service level data	30/05/2024
Independent Audit Report	06/11/2023	30/06/2024		31/07/2024
Compliance with working with children obligations	06/11/2023	30/06/2024		31/07/2024
Progress Report 3	01/05/2024	31/07/2024	Detailed contract expenditure, Service level data	30/08/2024
Progress Report 4	01/08/2024	31/10/2024	Detailed contract expenditure, Service level data	30/11/2024
Progress Report 5	01/11/2024	31/01/2025	Detailed contract expenditure, Service level data	28/02/2025
Progress Report 6	01/02/2025	30/04/2025	Detailed contract expenditure, Service level data	30/05/2025
Compliance with working with children obligations	01/07/2024	30/06/2025		31/07/2025

Report type	Period start date	Period end date	Agreed evidence	Due date
Independent Audit Report	01/07/2024	30/06/2025		31/07/2025
Progress Report 7	01/05/2025	31/07/2025	Detailed contract expenditure, Service level data	30/08/2025
Progress Report 8	01/08/2025	31/10/2025	Detailed contract expenditure, Service level data	30/11/2025
Progress Report 9	01/11/2025	31/01/2026	Detailed contract expenditure, Service level data	28/02/2026
Progress Report 10	01/02/2026	30/04/2026	Detailed contract expenditure, Service level data	30/05/2026
Independent Audit Report	01/07/2025	30/06/2026		31/07/2026
Compliance with working with children obligations	01/07/2025	30/06/2026		31/07/2026
End of project report	06/11/2023	31/07/2026	Detailed contract expenditure, Service level data, Independent audit report	29/10/2026

During the Agreement period, the Commonwealth may ask the Grantee for ad-hoc reports on the project. The Grantee must provide these reports in the timeframes notified by the Commonwealth.

F. Party representatives and address for notices

Grantee's representative and address

Grantee's representative name	s 47F
Position	Chief Operating Officer

Address	ANZ Building, Level 2 15 Moore Street Canberra ACT 2601
Business hours telephone	s 47F
Mobile	s 47F
Email	s 47F@cosboa.org.au

Commonwealth representative and address

Name of representative	s 47F
Position	Program Manager - Business Grants Hub
Postal address	GPO Box 2013 CANBERRA ACT 2601
Physical address	10 Binara Street CANBERRA ACT 2600
Business hours telephone	s 47F
Email	CyberWardens@industry.gov.au

The Parties' representatives will be responsible for liaison and the day-to-day management of the Grant, as well as accepting and issuing any written notices in relation to the Grant.

G. Activity Material

Not applicable

Supplementary Terms

ST1. Other Contributions

Not applicable

ST2. Activity Budget

ST2.1 In this Agreement, Appropriation means money drawn from the Consolidated Revenue Fund.

ST2.2 The Grantee agrees to use the Grant and any Other Contributions and undertake the Activity consistently with the Activity Budget in the following table:

Financial year 2023/24

Head of expenditure	Breakdown of expenditure	Agreed project cost
Project expenditure	s 47(1)(b)	
Project expenditure		
Project expenditure		
Project expenditure		
Project expenditure		
Project expenditure		
Project expenditure		
Project expenditure		
Project expenditure		
Financial year total		$6,604,000

Financial year 2024/25

Head of expenditure	Breakdown of expenditure	Agreed project cost
Project expenditure	s 47(1)(b)	
Project expenditure		
Project expenditure		
Project expenditure		
Project expenditure		
Project expenditure		

	s 47(1)(b)	
Project expenditure		
Project expenditure		
Project expenditure		
Financial year total		$8,369,000

Financial year 2025/26

Head of expenditure	Breakdown of expenditure	Agreed project cost
Project expenditure	s 47(1)(b)	
Project expenditure		
Project expenditure		
Project expenditure		
Project expenditure		
Project expenditure		
Project expenditure		
Project expenditure		
Project expenditure		
Financial year total		$8,021,750

Financial year 2026/27

Head of expenditure	Breakdown of expenditure	Agreed project cost
Project expenditure	s 47(1)(b)	
Project expenditure		
Project expenditure		
Project expenditure		
Project expenditure		
Project expenditure		
Project expenditure		

Project expenditure	s 47(1)(b)
Project expenditure	
Financial year total	$0

All financial years

Head of expenditure	Breakdown of expenditure	Agreed project cost
Project expenditure	s 47(1)(b)	
Project expenditure		
Project expenditure		
Project expenditure		
Project expenditure		
Project expenditure		
Project expenditure		
Project expenditure		
Project expenditure		
Project expenditure		
All financial years total		$22,994,750

Figures in the above table are GST inclusive amounts less GST credits that can be claimed in relation to the expenditure.

ST2.3 Subject to sufficient appropriation being available, the Grant will be paid up to the Annual Capped Amounts over the financial years specified in the following table.

Annual capped amounts

Financial Year	Annual capped amount (GST excl)
2023/24	$6,604,000
2024/25	$8,369,000
2025/26	$8,021,750
Total	$22,994,750

ST2.4 The Commonwealth is not required to make a payment if it would result in the amount paid in a financial year exceeding the Annual Capped Amount for that financial year specified in the table under clause ST2.3.

ST2.5 In accordance with the Activity Budget under clause ST2.2, the Annual Capped Amounts may not be exceeded unless the Commonwealth specifically approves an increase of that amount under clause ST2.8.

ST2.6 Subject to this clause, the Grantee may reallocate expenditure in respect of categories of expenditure in the Activity Budget, provided it does not materially change the Activity, any Milestone(s) set out in this Agreement, or cause the Grantee to be in breach of any of its obligations under this Agreement.

ST2.7 The Grantee must give the Commonwealth:

(a) at any time the Grantee wishes to request a variation to any one or more of the Annual Capped Amounts; or

(b) if otherwise requested by the Commonwealth,

a revised Activity Budget in a form acceptable to the Commonwealth. The revised Activity Budget must clearly identify any proposed changes, including of any proposed changes to the Annual Capped Amounts, and explain the reasons for the proposed changes.

ST2.8 The Commonwealth may, at its discretion, approve or reject a revised Activity Budget provided under clause ST2.7 and/or any proposed changes to the Annual Capped Amounts. The Commonwealth's approval may be granted subject to conditions.

ST2.9 If a revised Activity Budget and any proposed changes to the Annual Capped Amounts are approved by the Commonwealth, then it will become the Activity Budget and, if relevant, the Annual Capped Amounts will be adjusted accordingly.

ST3. Intellectual property in Activity Material

ST3.1 The Grantee agrees, on request from the Commonwealth, to provide the Commonwealth with a copy of any Activity Material in the format reasonably requested by the Commonwealth.

ST3.2 The Grantee agrees to provide the Commonwealth a permanent, non-exclusive, irrevocable, royalty-free licence (including a right to sub licence) to use, modify, communicate, reproduce, publish, and adapt the Activity Material as specified in the Grant Details for Commonwealth Purposes.

ST3.3 The Grantee warrants that the provision and use of Activity Material in accordance with the Agreement (and the use of specified Activity Material in accordance with ST3.2) will not infringe any third party's Intellectual Property Rights.

ST3.4 The Grantee will obtain written moral rights consents (other than in relation to acts of false attribution) from all authors of Reporting Material, and any Activity Material specified in the Grant Details, to the use of that Material by the Commonwealth in accordance with this Agreement, prior to that Material being provided to the Commonwealth.

ST4. Access/monitoring/inspection

ST4.1 The Grantee agrees to give the Commonwealth, or any persons authorised in writing by the Commonwealth:

(a) access to premises where the Activity is being performed and/or where Material relating to the Activity is kept within the time period specified in a Commonwealth notice; and

(b) permission to inspect and take copies of any Material relevant to the Activity.

ST4.2 The Auditor-General and any Information Officer under the *Australian Information Commissioner Act 2010* (Cth) (including their delegates) are persons authorised for the purposes of clause ST4.1.

ST4.3 This clause ST4 does not detract from the statutory powers of the Auditor-General or an Information Officer (including their delegates).

ST5. Equipment and Assets

Not applicable

ST6. Specified Personnel

Not applicable

ST7. Relevant qualifications, licences, permits, approvals or skills

Not applicable

ST8. Vulnerable Persons

Not applicable

ST9. Child safety

ST9.1 In this Agreement

Child	means an individual(s) under the age of 18 years and **Children** has a similar meaning;
Child-Related Personnel	means officers, employees, contractors (including subcontractors), agents and volunteers of the Grantee involved with the Activity who as part of that involvement may interact with Children;
Legislation	means a provision of a statute or subordinate legislation of the Commonwealth, or of a State, Territory or local authority;
National Principles for Child Safe Organisations	means the National Principles for Child Safe Organisations, which have been endorsed in draft form by the Commonwealth Government (available at: https://humanrights.gov.au/our-work/childrens-rights/projects/child-safe-organisations) and subsequently, from the time of their endorsement by the Council of Australian Governments, the final National Principles for Child Safe Organisations as published by the Australian Government;
Relevant Legislation	means Legislation in force in any jurisdiction where any part of the Activity may be carried out;
Working With Children Check or WWCC	means the process in place pursuant to Relevant Legislation to screen an individual for fitness to work with Children.

Relevant checks and authority

ST9.2 The Grantee must

(a) comply with all Relevant Legislation relating to the employment or engagement of Child-Related Personnel in relation to the Activity, including all necessary Working With Children Checks however described;

(b) ensure that Working With Children Checks obtained in accordance with this clause ST9.2 remain current and that all Child-Related Personnel continue to comply with all Relevant Legislation for the duration of their involvement in the Activity; and

(c) ensure that any subcontract entered into by the Grantee for the purposes of this Agreement imposes the same obligations in clauses ST9.2(a) and (b) on the subcontractor and also requires the subcontractor to include those obligations in any secondary subcontracts.

National Principles for Child Safe Organisations and other action for the safety of Children

ST9.3 The Grantee agrees in relation to the Activity to:

(a) implement the National Principles for Child Safe Organisations;

(b) ensure that all Child-Related Personnel implement the National Principles for Child Safe Organisations;

(c) complete and update, at least annually, a risk assessment to identify the level of responsibility for Children and the level of risk of harm or abuse to Children;

(d) put into place and update, at least annually, an appropriate risk management strategy to manage risks identified through the risk assessment required by this clause ST9.3;

(e) provide training and establish a compliance regime to ensure that all Child Related Personnel are aware of, and comply with

(i) the National Principles for Child Safe Organisations;

(ii) the Grantee's risk management strategy required by this clause ST9.3;

(iii) Relevant Legislation relating to requirements for working with Children, including Working With Children Checks;

(iv) Relevant Legislation relating to mandatory reporting of suspected child abuse or neglect, however described;

(f) provide the Commonwealth with an annual statement of compliance with clauses ST9.2 and ST9.3, in such form as may be specified by the Commonwealth; and

(g) ensure that any subcontract entered into by the Grantee for the purposes of this Agreement imposes the same obligations in clauses ST9.3(a) to (e) on the subcontractor and also requires the subcontractor to include those obligations in any secondary subcontracts.

ST9.4 With reasonable notice to the Grantee, the Commonwealth may conduct a review of the Grantee's compliance with this clause ST9.

ST9.5 The Grantee agrees to:

(a) notify the Commonwealth of any failure to comply with this clause ST9;

(b) co-operate with the Commonwealth in any review conducted by the Commonwealth of the Grantee's implementation of the National Principles for Child Safe Organisations or compliance with this clause ST9; and

(c) promptly, and at the Grantee's cost, take such action as is necessary to rectify, to the Commonwealth's satisfaction, any failure to implement the National Principles for Child Safe Organisations or any other failure to comply with this clause ST9.

ST10. Commonwealth Material, facilities and assistance

Not applicable

ST11. Jurisdiction

ST11.1 This Agreement is governed by the law of the Australian Capital Territory.

ST12. Grantee trustee of trust (if applicable)

ST12.1 In this Agreement, **Trust** means the trust specified in the Parties to the Agreement section of this Agreement.

ST12.2 The Grantee warrants that:

(a) it is the sole trustee of the Trust; and

(b) it has full and valid power and authority to enter into this Agreement and perform the obligations under it on behalf of the Trust; and

(c) it has entered into this Agreement for the proper administration of the Trust; and

(d) all necessary resolutions, consents, approvals and procedures have been obtained or duly satisfied to enter into this Agreement and perform the obligations under it; and

(e) it has the right to be indemnified out of the assets of the Trust for all liabilities incurred by it under this Agreement.

ST13. Fraud

ST13.1 In this Agreement, Fraud means dishonestly obtaining a benefit, or causing a loss, by deception or other means, and includes alleged, attempted, suspected or detected fraud.

ST13.2 The Grantee must ensure its personnel and subcontractors do not engage in any Fraud in relation to the Activity.

ST13.3 If the Grantee becomes aware of:

(a) any Fraud in relation to the performance of the Activity; or

(b) any other Fraud that has had or may have an effect on the performance of the Activity;

then it must within 5 business days report the matter to the Commonwealth and all appropriate law enforcement and regulatory agencies.

ST13.4 The Grantee must, at its own cost, investigate any Fraud referred to in clause ST13.3 in accordance with the Australian Government Investigations Standards available at www.ag.gov.au.

ST13.5 The Commonwealth may, at its discretion, investigate any Fraud in relation to the Activity. The Grantee agrees to co-operate and provide all reasonable assistance at its own cost with any such investigation.

ST13.6 This clause survives the termination or expiry of the Agreement.

ST14. Prohibited dealings

Not applicable

ST15. Anti-corruption

ST15.1 In this Agreement:

Illegal or Corrupt Practice means directly or indirectly:

(a) making or causing to be made, any offer, gift, payment, consideration or benefit of any kind to any party, or

(b) receiving or seeking to receive, any offer, gift, payment, consideration or benefit of any kind from any party, as an inducement or reward in relation to the performance of the Activity, which would or could be construed as an illegal or corrupt practice.

ST15.2 The Grantee warrants that the Grantee, its officers, employees, contractors, agents and any other individual or entity involved in carrying out the Activity have not, engaged in an Illegal or Corrupt Practice.

ST15.3 The Grantee agrees not to, and to take all reasonable steps to ensure that its officers, employees, contractors, agents and any other individual or entity involved in carrying out the Activity do not:

(a) engage in an Illegal or Corrupt Practice; or

(b) engage in any practice that could constitute the offence of bribing a foreign public official contained in section 70.2 of the Criminal Code Act 1995 (Cth).

ST15.4 The Grantee agrees to inform the Commonwealth within five business days if the Grantee becomes aware of any activity as described in ST15.3 in relation to the performance of the Activity.

ST16. Step-in rights

Not applicable

ST17. Grant administrator

Not applicable

ST18. Management Adviser

Not applicable

ST19. Indemnities

ST19.1 The Grantee indemnifies the Commonwealth, its officers, employees and contractors against any claim, loss or damage arising in connection with the Activity.

ST19.2 The Grantee's obligation to indemnify the Commonwealth will reduce proportionally to the extent any act or omission involving fault on the part of the Commonwealth contributed to the claim, loss or damage.

ST20. Compliance with Legislation and Policies

ST20.1 In this Agreement:

Legislation means a provision of a statute or subordinate legislation of the Commonwealth, or of a State, Territory or local authority.

ST20.2 The Grantee agrees to comply with all Legislation applicable to its performance of this Agreement.

ST20.3 The Grantee agrees, in carrying out its obligations under this Agreement, to comply with any of the Commonwealth's policies as notified, referred or made available by the Commonwealth to the Grantee (including by reference to an internet site).

ST20.4 In carrying out the Activity, the Grantee must comply with the following applicable policies/laws:

(a) All State, Territory or Commonwealth law relating to the employment or engagement of people who work or volunteer with children in relation to the Activity including mandatory reporting and working with children checks however described and, if requested, provide the Commonwealth, at the Grantee's cost, with an annual statement of compliance with these requirements in such form as may be specified by the Commonwealth.

ST21. Work health and safety

ST21.1 The Grantee agrees to ensure that it complies at all times with all applicable work health and safety legislative and regulatory requirements and any additional work health and safety requirements set out in the Grant Details.

ST21.2 If requested by the Commonwealth, the Grantee agrees to provide copies of its work health and safety management plans and processes and such other details of the arrangements it has in place to meet the requirements referred to in clause ST21.1.

ST21.3 When using the Commonwealth's premises or facilities, the Grantee agrees to comply with all reasonable directions and procedures relating to work health and safety and security in effect at those premises or facilities, as notified by the Commonwealth or as might reasonably be inferred from the use to which the premises or facilities are being put.

ST22. Transition

Not applicable

ST23. Corporate Governance

ST23.1 In this Agreement:

Constitution means (depending on the context):

(a) a company's, body corporate's or incorporated association's constitution, or equivalent documents, which (where relevant) includes rules and any amendments that are part of the constitution;

(b) in relation to any other kind of body:

(i) the body's charter or memorandum; or

(ii) any instrument or law constituting or defining the constitution of the body or governing the activities of the body or its members.

ST23.2 The Grantee warrants that nothing in its constitution conflicts with its obligations under this Agreement.

ST23.3 The Grantee agrees to provide a copy of its constitution to the Commonwealth upon request and inform the Commonwealth whenever there is a change in the Grantee's constitution, structure or management.

ST24. Counterparts

ST24.1 This Agreement may be executed in any number of counterparts. All counterparts, taken together, constitute one instrument. A Party may execute this Agreement by signing any counterpart.

ST25. Secret and Sacred Indigenous Material

Not applicable

ST26. Australian Industry Participation plan, Executive Summary and Implementation Report(s)

Not applicable

Schedule 1: Commonwealth Standard Grant Conditions

1. Undertaking the Activity

1.1 The Grantee agrees to undertake the Activity for the purpose of the Grant in accordance with this Agreement.

1.2 The Grantee is fully responsible for the Activity and for ensuring the performance of all its obligations under this Agreement in accordance with all relevant laws. The Grantee will not be relieved of that responsibility because of:

(a) the grant or withholding of any approval or the exercise or non-exercise of any right by the Commonwealth; or

(b) any payment to, or withholding of any payment from, the Grantee under this Agreement.

1.3 The Grantee agrees that for the term of this Agreement, the Grantee will continue to meet the eligibility obligations relating to the National Redress Scheme[1] set out under the relevant grant opportunity guidelines to receive the Grant.

2. Payment of the Grant

2.1 The Commonwealth agrees to pay the Grant to the Grantee in accordance with the Grant Details.

2.2 Notwithstanding any other provision of this Agreement, the Commonwealth may by notice withhold payment of any amount of the Grant and/or take any other action specified in the Supplementary Terms if it reasonably believes that:

(a) the Grantee has not complied with this Agreement;

(b) the Grantee is unlikely to be able to perform the Activity or manage the Grant in accordance with this Agreement; or

(c) there is a serious concern relating to this Agreement that requires investigation.

2.3 A notice under clause 2.2 will contain the reasons any action taken under clause 2.2 and, where relevant, the steps the Grantee can take to address those reasons.

2.4 The Commonwealth will only be obliged to pay the withheld amount once the Grantee has addressed the reasons contained in a notice under clause 2.2 to the Commonwealth's reasonable satisfaction.

3. Acknowledgements

3.1 The Grantee agrees not to make any public announcement, including by social media, in connection with the awarding of the Grant without the Commonwealth's prior written approval.

3.2 The Grantee agrees to acknowledge the Commonwealth's support in all Material, publications and promotional and advertising materials published in connection with this Agreement. The Commonwealth may notify the Grantee of the form of acknowledgement that the Grantee is to use.

[1] The National Redress Scheme can be found at https://www.nationalredress.gov.au

4. Notices

4.1 Each Party agrees to promptly notify the other Party of anything reasonably likely to adversely affect the undertaking of the Activity, management of the Grant or its performance of any of its other requirements under this Agreement.

4.2 A notice given by a Party under this Agreement must be in writing and addressed to the other Party's representative as set out in the Grant Details or as most recently updated by notice given in accordance with this clause.

5. Relationship between the Parties

5.1 A Party is not by virtue of this Agreement the employee, agent or partner of the other Party and is not authorised to bind or represent the other Party.

6. Subcontracting

6.1 The Grantee is responsible for the performance of its obligations under this Agreement, including in relation to any tasks undertaken by subcontractors.

6.2 The Grantee agrees to make available to the Commonwealth the details of any of its subcontractors engaged to perform any tasks in relation to this Agreement upon request.

7. Conflict of interest

7.1 Other than those which have already been disclosed to the Commonwealth, the Grantee warrants that, to the best of its knowledge, at the date of this Agreement, neither it nor its officers have any actual, perceived or potential conflicts of interest in relation to the Activity.

7.2 If during the term of the Agreement, any actual, perceived or potential conflict arises or there is any material change to a previously disclosed conflict of interest, the Grantee agrees to:

(a) notify the Commonwealth promptly and make full disclosure of all relevant information relating to the conflict; and

(b) take any steps the Commonwealth reasonably requires to resolve or otherwise deal with that conflict.

8. Variation, assignment and waiver

8.1 This Agreement may be varied in writing only, signed by both Parties.

8.2 The Grantee cannot assign its obligations, and agrees not to assign its rights, under this Agreement without the Commonwealth's prior approval.

8.3 The Grantee agrees not to enter into negotiations with any other person for the purposes of entering into an arrangement that will require novation of, or involve any assignment of rights under, this Agreement without first consulting the Commonwealth.

8.4 A waiver by a Party of any of its rights under this Agreement is only effective if it is in a signed written notice to the other Party and then only to the extent specified in that notice.

9. Taxes, duties and government charges

9.1 The Grantee agrees to pay all taxes, duties and government charges imposed or levied in Australia or overseas in connection with the performance of this Agreement, except as provided by this Agreement.

9.2 If Goods and Services Tax (GST) is payable by a supplier on any supply made under this Agreement, the recipient of the supply will pay to the supplier an amount equal to the GST payable on the supply, in addition to and at the same time that the consideration for the supply is to be provided under this Agreement.

9.3 The Parties acknowledge and agree that they each:

(a) are registered for GST purposes;

(b) have quoted their Australian Business Number to the other; and

(c) must notify the other of any changes to the matters covered by this clause.

9.4 The Grantee agrees that the Commonwealth will issue it with a recipient created tax invoice for any taxable supply it makes under this Agreement.

9.5 The Grantee agrees not to issue tax invoices in respect of any taxable supplies.

9.6 If the Grantee is not, or not required to be, registered for GST, then:

(a) clauses 9.3(a), 9.4 and 9.5 do not apply; and

(b) the Grantee agrees to notify the Commonwealth in writing within 7 days of becoming registered for GST if during the term of the Agreement it becomes, or is required to become, registered for GST.

10. Spending the Grant

10.1 The Grantee agrees to spend the Grant for the purpose of performing the Activity and otherwise in accordance with this Agreement.

10.2 Within 90 days after the Activity Completion Date, the Grantee agrees to provide the Commonwealth with an independently audited financial acquittal report verifying that the Grant has been spent in accordance with this Agreement.

10.3 The reports under clause 10.2 must be audited by:

(a) a Registered Company Auditor registered under the *Corporations Act 2001* (Cth); or

(b) a certified Practising Accountant; or

(c) a member of the Institute of Public Accountants; or

(d) a member of Chartered Accountants Australia and New Zealand;

who is not a principal member, shareholder, officer or employee of the Grantee or a related body corporate.

11. Repayment

11.1 If any amount of the Grant:

(a) has been spent other than in accordance with this Agreement; or

(b) is additional to the requirements of the Activity

then the Commonwealth may, by written notice:

(c) require the Grantee to repay that amount to the Commonwealth;

(d) require the Grantee to deal with that amount as directed by the Commonwealth; or

(e) deduct the amount from subsequent payments of the Grant or amounts payable under another agreement between the Grantee and the Commonwealth.

11.2 If the Commonwealth issues a notice under this Agreement requiring the Grantee to repay a Grant amount:

(a) the Grantee must do so within the time period specified in the notice;

(b) the Grantee must pay interest on any part of the amount that is outstanding at the end of the time period specified in the notice until the outstanding amount is repaid in full; and

(c) the Commonwealth may recover the amount and any interest under this Agreement as a debt due to the Commonwealth without further proof of the debt being required.

12. Record keeping

12.1 The Grantee agrees to keep financial accounts and other records that:

(a) detail and document the conduct and management of the Activity;

(b) identify the receipt and expenditure of the Grant and any Other Contributions separately within the Grantee's accounts and records so that at all times the Grant is identifiable;

(c) enable all receipts and payments related to the Activity to be identified and reported.

12.2 The Grantee agrees to keep the records for five years after the Activity Completion Date or such other time specified in the Grant Details and provide copies of the records to the Commonwealth upon request.

13. Reporting and liaison

13.1 The Grantee agrees to provide the Reporting Material specified in the Grant Details to the Commonwealth.

13.2 In addition to the obligations in clause 13.1, the Grantee agrees to:

(a) liaise with and provide information to the Commonwealth as reasonably required by the Commonwealth; and

(b) comply with the Commonwealth's reasonable requests, directions, or monitoring requirements,

in relation to the Activity.

13.3 If the Commonwealth acting reasonably has concerns regarding the performance of the Activity or the management of the Grant, the Commonwealth may by written notice require the Grantee to provide one or more additional reports, containing the information and by the date(s) specified in the notice.

13.4 The Grantee acknowledges that the giving of false or misleading information to the Commonwealth is a serious offence under the *Criminal Code Act 1995* (Cth).

14. Privacy

14.1 When dealing with Personal Information in carrying out the Activity, the Grantee agrees:

(a) to comply with the requirements of the *Privacy Act 1988* (Cth);

(b) not to do anything which, if done by the Commonwealth, would be a breach of an Australian Privacy Principle;

(c) to ensure that any of the Grantee's subcontractors or personnel who deal with Personal Information for the purposes of this Agreement are aware of the requirements of the *Privacy Act 1988* (Cth) and the Grantee's obligations under this clause;

(d) to immediately notify the Commonwealth if the Grantee becomes aware of an actual or possible breach of this clause by the Grantee or any of the Grantee's subcontractors or personnel.

14.2 In carrying out the Activity, the Grantee agrees not to send any Personal Information outside of Australia without the Commonwealth's prior written approval. The Commonwealth may impose any conditions it considers appropriate when giving its approval.

15. Confidentiality

15.1 The Parties agree not to disclose each other's confidential information without the other Party's prior written consent unless required or authorised by law or Parliament to disclose.

15.2 The Commonwealth may disclose the Grantee's confidential information where;

(a) the Commonwealth is providing information about the Activity or Grant in accordance with Commonwealth accountability and reporting requirements;

(b) the Commonwealth is disclosing the information to a Minister of the Australian Government, a House or Committee of the Commonwealth Parliament; or

(c) the Commonwealth is disclosing the information to its personnel or another Commonwealth agency where this serves the Commonwealth's legitimate interests.

16. Insurance

16.1 The Grantee agrees to maintain adequate insurance for as long as any obligations remain in connection with this Agreement and provide proof of insurance to the Commonwealth upon request.

16.2 The Grantee agrees to provide proof of insurance to the Commonwealth upon request and within the time specified in the request.

17. Intellectual property

17.1 Subject to clause 17.2, the Grantee owns the Intellectual Property Rights in Activity Material and Reporting Material.

17.2 This Agreement does not affect the ownership of Intellectual Property Rights in Existing Material.

17.3 The Grantee provides the Commonwealth a permanent, non-exclusive, irrevocable, royalty-free licence to use, modify, communicate, reproduce, publish, adapt and sub-license the Reporting Material for Commonwealth Purposes.

17.4 The licence in clause 17.3 does not apply to Activity Material.

18. Dispute resolution

18.1 The Parties agree not to initiate legal proceedings in relation to a dispute arising under this Agreement unless they have first tried and failed to resolve the dispute by negotiation.

18.2 Unless clause 18.3 applies, the Parties agree to continue to perform their respective obligations under this Agreement when a dispute exists.

18.3 The Parties may agree to suspend performance of the Agreement pending resolution of the dispute.

18.4 Failing settlement by negotiation in accordance with clause 18.1, the Parties may agree to refer the dispute to an independent third person with power to intervene and direct some form of resolution, in which case the Parties will be bound by that resolution. If the Parties do not agree to refer the dispute to an independent third person, either Party may initiate legal proceedings.

18.5 Each Party will bear their own costs in complying with this clause 18, and the Parties will share equally the cost of any third person engaged under clause 18.4.

18.6 The procedure for dispute resolution under this clause does not apply to any action relating to termination, cancellation or urgent interlocutory relief.

19. Reduction, Suspension and Termination

19.1 Reduction in scope of agreement for fault

19.1.1 If the Grantee does not comply with an obligation under this Agreement and the Commonwealth believes that the non-compliance is incapable of remedy, or if the Grantee has failed to comply with a notice to remedy, the Commonwealth may by written notice reduce the scope of the Agreement.

19.1.2 The Grantee agrees, on receipt of the notice of reduction, to:

(a) stop or reduce the performance of the Grantee's obligations as specified in the notice;

(b) take all available steps to minimise loss resulting from the reduction;

(c) continue performing any part of the Activity or the Agreement not affected by the notice if requested to do so by the Commonwealth;

(d) report on, and return any part of the Grant to the Commonwealth, or otherwise deal with the Grant, as directed by the Commonwealth.

19.1.3 In the event of reduction under clause 19.1.1, the amount of the Grant will be reduced in proportion to the reduction in the scope of the Agreement.

19.2 Suspension

19.2.1 If:

(a) the Grantee does not comply with an obligation under this Agreement and the Commonwealth believes that the non-compliance is capable of remedy;

(b) the Commonwealth reasonably believes that the Grantee is unlikely to be able to perform the Activity or manage the Grant in accordance with this Agreement; or

(c) the Commonwealth reasonably believes that there is a serious concern relating to this Agreement that requires investigation;

the Commonwealth may by written notice:

(d) immediately suspend the Grantee from further performance of the Agreement (including expenditure of the Grant); and/or

(e) require that the non-compliance or inability be remedied, or the investigation be completed, within the time specified in the notice.

19.2.2 If the Grantee:

(a) remedies the non-compliance or inability specified in the notice to the Commonwealth's reasonable satisfaction, or the Commonwealth reasonably concludes that the concern is unsubstantiated, the Commonwealth may direct the Grantee to recommence performing the Activity; or

(b) fails to remedy the non-compliance or inability within the time specified, or the Commonwealth reasonably concludes that the concern is likely to be substantiated, the Commonwealth may reduce the scope of the Agreement in accordance with clause 19.1 or terminate the Agreement immediately by giving a second notice in accordance with clause 19.3.

19.3 Termination for fault

19.3.1 The Commonwealth may terminate this Agreement by notice where the Grantee has:

(a) failed to comply with an obligation under this Agreement and the Commonwealth believes that the non-compliance is incapable of remedy or where clause 19.2.2(b) applies; or

(b) provided false or misleading statements in relation to the Grant; or

(c) become bankrupt or insolvent, entered into a scheme of arrangement with creditors, or come under any form of external administration; or

(d) in addition to clause 19.3.1(a), breached the requirements in subclause 1.3.

19.3.2 The Grantee agrees, on receipt of the notice of termination, to:

(a) stop the performance of the Grantee's obligations;

(b) take all available steps to minimise loss resulting from the termination; and

(c) report on, and return any part of the Grant to the Commonwealth, or otherwise deal with the Grant, as directed by the Commonwealth.

20. Cancellation or reduction for convenience

20.1 The Commonwealth may cancel or reduce the scope of this Agreement by notice, due to:

(a) a change in government policy; or

(b) a Change in the Control of the Grantee which the Commonwealth reasonably believes will negatively affect the Grantee's ability to comply with this Agreement.

20.2 On receipt of a notice of reduction or cancellation under this clause, the Grantee agrees to:

(a) stop or reduce the performance of the Grantee's obligations as specified in the notice; and

(b) take all available steps to minimise loss resulting from that reduction or cancellation; and

(c) continue performing any part of the Activity or the Agreement not affected by the notice if requested to do so by the Commonwealth;

(d) report on, and return any part of the Grant to the Commonwealth, or otherwise deal with the Grant, as directed by the Commonwealth.

20.3 In the event of reduction or cancellation under this clause, the Commonwealth will be liable only to:

(a) pay any part of the Grant due and owing to the Grantee under this Agreement at the date of the notice; and

(b) reimburse any reasonable and substantiated expenses the Grantee unavoidably incurs that relate directly and entirely to the reduction in scope or cancellation of the Agreement.

20.4 In the event of reduction, the amount of the Grant will be reduced in proportion to the reduction in the scope of the Agreement.

20.5 The Commonwealth's liability to pay any amount under this clause is:

(a) subject to the Grantee's compliance with this Agreement; and

(b) limited to an amount that when added to all other amounts already paid under the Agreement will not exceed the total amount of the Grant.

20.6 The Grantee will not be entitled to compensation for loss of prospective profits or benefits that would have been conferred on the Grantee but for the cancellation or reduction in scope of the Agreement under clause 20.1.

20.7 The Commonwealth will act reasonably in exercising its rights under this clause.

21. Survival

21.1 The following clauses survive termination, cancellation or expiry of this Agreement:

- clause 10 (Spending the Grant);
- clause 11 (Repayment);
- clause 12 (Record keeping);
- clause 13 (Reporting and liaison);
- clause 14 (Privacy);
- clause 15 (Confidentiality);
- clause 16 (Insurance);
- clause 17 (Intellectual property);
- clause 19 (Reduction, Suspension and Termination);
- clause 21 (Survival);
- clause 22 (Definitions);
- ST3 (Intellectual property in Activity Material);
- ST4 (Access/monitoring/inspection);
- ST19 (Indemnities); and
- any other clause which expressly or by implication from its nature is meant to survive.

22. Definitions

22.1 In this Agreement, unless the contrary appears:

- **Activity** means the activities described in the Grant Details and includes the provisions of the Reporting Material.
- **Activity Completion Date** means the date or event specified in the Grant Details.
- **Activity Material** means any Material, other than Reporting Material, created or developed by the Grantee as a result of the Activity and includes any Existing Material that is incorporated in or supplied with the Activity Material.
- **Agreement** means the Grant Details, Supplementary Terms (if any), the Commonwealth Standard Grant Conditions and any other document referenced or incorporated in the Grant Details.
- **Agreement End Date** means the date or event specified in the Grant Details.
- **Australian Privacy Principle** has the same meaning as in the *Privacy Act 1988.*
- **Change in the Control** means any change in any person(s) who directly exercise effective control over the Grantee.
- **Commonwealth** means the Commonwealth of Australia as represented by the Commonwealth entity specified in the Agreement and includes, where relevant, its officers, employees, contractors and agents.
- **Commonwealth Purposes** includes the following:

  (a) the Commonwealth verifying and assessing grant proposals, including a grant application;

  (b) the Commonwealth administering, monitoring, reporting on, auditing, publicising and evaluating a grant program or exercising its rights under this Agreement;

  (c) the Commonwealth preparing, managing, reporting on, auditing and evaluating agreements, including this Agreement; and

  (d) the Commonwealth developing and publishing policies, programs, guidelines and reports, including Commonwealth annual reports;

  but in all cases:

  (e) excludes the commercialisation (being for-profit use) of the Material by the Commonwealth.
- **Commonwealth Standard Grant Conditions** means this document.
- **Existing Material** means Material developed independently of this Agreement that is incorporated in or supplied as part of Reporting Material or Activity Material.
- **Grant** means the money, or any part of it, payable by the Commonwealth to the Grantee for the Activity as specified in the Grant Details and includes any interest earned by the Grantee on that money once the Grant has been paid to the Grantee.
- **Grantee** means the legal entity other than the Commonwealth specified in the Agreement and includes, where relevant, its officers, employees, contractors and agents.
- **Grant Details** means the document titled Grant Details that forms part of this Agreement.
- **Intellectual Property Rights** means all copyright, patents, registered and unregistered trademarks (including service marks), registered designs, and other rights resulting from intellectual activity (other than moral rights under the *Copyright Act 1968*).
- **Material** includes documents, equipment, software (including source code and object code versions), goods, information and data stored by any means including all copies and extracts of them.

- **Party** means the Grantee or the Commonwealth.
- **Personal Information** has the same meaning as in the *Privacy Act 1988*.
- **Records** includes documents, information and data stored by any means and all copies and extracts of the same.
- **Reporting Material** means all Material which the Grantee is required to provide to the Commonwealth for reporting purposes as specified in the Grant Details, and includes any Existing Material that is incorporated in or supplied with the Reporting Material.

Signatures

Executed as an agreement: s 47F

Commonwealth

Signed for and on behalf of the Commonwealth of Australia as represented by the Department of Industry, Science and Resources.

Name	Noel Taloni
Position	Acting General Manager Business Grants Hub
Date	6 November 2023

Grantee

Full legal name of the Grantee	COUNCIL OF SMALL BUSINESS ORGANISATIONS OF AUSTRALIA LIMITED ABN: 43008597304
Name of Authorised Representative	s 47F
Date	03/11/2023

Schedule 2 Reporting requirements

Appendix 1

Small Business Cyber Wardens - progress report requirements

You will need to provide the following information in your progress reports. The Commonwealth reserves the right to amend or adjust the requirements.

You must complete and submit your report on the business.gov.au portal. You can enter the required information in stages and submit when it is complete.

Project progress

a. Complete the following table, updating for all milestones shown in the Activity Schedule of your grant agreement.

Milestone	Agreed end date	Actual/ anticipated end date	Current % complete	Progress comments – work undertaken and impact of any delay

b. Where applicable, describe any project activities completed during the reporting period that are not captured in the table above.

c. Is the overall project proceeding in line with your grant agreement?

If no, identify any changes or anticipated issues. Comment on any impacts on project timing and outcomes and how you expect to manage these.

d. Are there any planned events relating to the project that you are required to notify us about in accordance with your agreement?

If yes, provide details of the event including date, time, purpose of the event and key stakeholders expected to attend.

Project outcomes

a. Outline the project outcomes achieved to date.

Project expenditure

Provide the following information about your eligible project expenditure. Eligible expenditure is divided into the same categories as the budget in your application.

If you are registered for GST, enter the GST exclusive amount. If you are not registered for GST, enter the GST inclusive amount. We may ask you to provide evidence of costs incurred.

Refer to the grant opportunity guidelines or contact us if you have any questions about eligible expenditure.

a. What is the eligible expenditure you have incurred in this reporting period?

b. What is the estimated eligible expenditure for the next reporting period?

c. What is the estimated eligible expenditure for remaining reporting periods in current financial year (if applicable)?

d. What is the estimated total eligible expenditure for future financial years?

e. What is the estimated total eligible expenditure for the project?

f. Briefly explain the reason for any changes between the forecast and actual expenditure for the current reporting period, and any significant changes to the forecast budget for the remainder of the project.

g. Is the project expenditure broadly in line with the activity budget in the grant agreement?

If no, explain the reasons.

Attachments

a. Attach agreed data relating to:

- small businesses engaged and individuals enrolled, certified and re-certified through your program each quarter
- research, awareness and education campaigns conducted throughout the quarter.

b. Attach any agreed evidence required with this report to demonstrate project progress.

c. Attach copies of any published reports and promotional material, relating to the project.

Declaration

You must ensure an authorised person completes the report and can declare the following:

- The information in this report is accurate, complete and not misleading and that I understand the giving of false or misleading information is a serious offence under the *Criminal Code 1995* (Cth).
- The activities identified in this report are for the purposes stated in the grant agreement.
- I am aware of the grantee's obligations under their grant agreement, including the need to keep the Commonwealth informed of any circumstances that may impact on the objectives, completion and/or outcomes of the agreed project.
- I am aware that the grant agreement empowers the Commonwealth to terminate the grant agreement and to request repayment of funds paid to the grantee where the grantee is in breach of the grant agreement.

Appendix 2

Small Business Cyber Wardens - end of project report requirements

You will need to provide the following information in your end of project report. The Commonwealth reserves the right to amend or adjust the requirements.

You must complete and submit your report on the business.gov.au portal. You can enter the required information in stages and submit when it is complete.

Project achievements

a. Complete the following table, updating for all milestones shown in the Activity Schedule of your grant agreement.

Milestone	Agreed end date	Actual/ anticipated end date	Current % complete	Progress comments – work undertaken and impact of any delay

b. Where applicable, describe any project activities completed during the reporting period that are not captured in the table above.

Project outcomes

a. Outline the project outcomes achieved by the project end date.

b. Do the achieved project outcomes align with those specified in the grant agreement?

If no, explain why.

c. Are there any planned events relating to the project that you are required to notify us about in accordance with your agreement?

If yes, provide details of the event including date, time, purpose of the event and key stakeholders expected to attend.

Project benefits

a. What benefits has the project achieved?

b. What ongoing impact will the project have?

c. Did the project result in any unexpected benefits?

If yes, explain why.

d. Did the project result in any unexpected negative impacts?

If yes, explain why.

e. Is there any other information you wish to provide about your project?

If yes, provide details.

Total eligible project expenditure

a. Indicate the total eligible project expenditure incurred. Eligible expenditure is divided into the same categories as the budget in your application.

If you are registered for GST, enter the GST exclusive amount. If you are not registered for GST, enter the GST inclusive amount. We may ask you to provide evidence of costs incurred.

Refer to the grant opportunity guidelines or contact us if you have any questions about eligible expenditure.

b. Provide any comments you may have to clarify any figures.

c. Was the expenditure incurred in accordance with the activity budget in the grant agreement?

If no, explain the reason for a project underspend or overspend, or any other significant changes to the budget.

Updated business indicators

a. Provide the following financial data for your organisation for your latest complete financial year.

These fields are mandatory and entering $0 is acceptable if applicable.

- Financial year completed
- Sales revenue (turnover)
- Export revenue
- R&D expenditure
- Taxable income
- Number of employees including working proprietors and salaried directors (headcount)
- Number of independent contractors (headcount)

Attachments

a. Attached agreed data in relation to:

- small businesses engaged and individuals enrolled, certified and re-certified through your program
- research, awareness and education campaigns conducted throughout the project.

b. Attach any agreed evidence required with this report to demonstrate progress or successful completion of your project.

c. Attach copies of any published reports and promotional material, relating to the project.

Declaration

You must ensure an authorised person completes the report and can declare the following:

- The information in this report is accurate, complete and not misleading and that I understand the giving of false or misleading information is a serious offence under the *Criminal Code 1995* (Cth).
- The grant was spent in accordance with the grant agreement.
- I am aware of the grantee's obligations under their grant agreement, including survival clauses.
- I am aware that the grant agreement empowers the Commonwealth to terminate the grant agreement and to request repayment of funds paid to the grantee where the grantee is in breach of the grant agreement.

Appendix 3

Independent audit report

Background

These templates assist Grantees (and their auditors) to understand the audit requirements under a Commonwealth grant agreement administered by the Department of Industry, Science and Resources. For further information contact us on 13 28 46 or at business.gov.au.

When an independent audit report is required under our grant agreements the Grantee must provide us with:

- a statement of grant income and expenditure against the expenditure categories under the grant agreement (attachment A)
- an independent audit report on the statement of grant income and expenditure (attachment B)
- certification of certain matters by the auditor (attachment C).

You can find additional information on the grant opportunity relevant to your grant at business.gov.au or by calling us on 13 28 46.

Eligible expenditure

Advice on eligible expenditure for projects under the grant opportunity can be found in grant opportunity guidelines. These guidelines are revised from time to time and therefore more than one version of the document may exist. The relevant guidelines are those that were effective at the time the Grantee's application was accepted.

It is essential that Grantees and their auditors understand the eligible expenditure requirements because these determine whether, and the extent to which, certain costs are reportable and claimable.

The amount of grant funding we approve is based on the Grantee's estimated eligible expenditure, as provided in their application. However, the grant funding any Grantee is ultimately entitled to receive is determined against actual eligible expenditure incurred and paid for on the project. The grant amount specified in the grant agreement is the **maximum** amount the Grantee may be paid.

The expenditure reported in the 'statement of grant income and expenditure' at attachment A must represent actual 'eligible expenditure' paid on the project during that period.

Attachment A – Statement of grant income and expenditure

Grant opportunity name	[grant opportunity name]
Project number	[project number]
Grantee	[organisation]
Project title	[project title]
Reporting period start date	[project start date or other reporting period start date]
Reporting period end date	[project end date or other reporting period end date]

This statement of grant income and expenditure must be prepared by the Grantee and contain the following:

- Statement of funds, Grantee contributions and other financial assistance*
- Statement of eligible expenditure*
- Notes to the statement of eligible expenditure, explaining the basis of compilation
- Certification by directors of the Grantee
- *We will compare this information to that detailed in the grant agreement.

1. Statement of funds, Grantee contributions and other financial assistance

Complete the following table for all cash [and in-kind] contributions for your project for the period in question, including:

- the grant
- other government funding
- your own contributions
- partner or other third party contributions
- any additional private sector funding.

Insert rows as required.

Contributor	Cash amount (GST excl)	[Estimated in-kind amount (GST excl)]	Total (GST excl)
Grant	$[enter amount]	$[enter amount]	$[enter amount]
Grantee	$[enter amount]	$[enter amount]	$[enter amount]
[enter contributor]	$[enter amount]	$[enter amount]	$[enter amount]
[enter contributor]	$[enter amount]	$[enter amount]	$[enter amount]
Total	$[enter amount]	$[enter amount]	$[enter amount]

2. Statement of eligible expenditure

You must provide detail of the eligible expenditure that has been incurred and paid for during the reporting period in a 'Statement of eligible expenditure' that contains the following information.

No. of expenditure item	Eligible expenditure category (as per grant agreement)	Eligible expenditure item	Supplier name	Supplier invoice number	Supplier invoice date	Invoice amount GST exclusive	Date invoice paid (if applicable)

Comment on any variance between the expenditure items and amounts detailed in the grant agreement and the actual items and amounts detailed in the attached statement of eligible expenditure.

[enter details]

3. Note to the statement of eligible expenditure

3.1 Eligible expenditure

The eligible expenditure as reported in the statement of eligible expenditure is in accordance with the grant opportunity guidelines.

3.2 Basis of compilation

This statement of eligible expenditure has been prepared to meet the requirements of the grant agreement between [enter Grantee name] and the Commonwealth represented by the Department of Industry, Science and Resources. Significant accounting policies applied in the compilation of the statement of grant income and expenditure include the following:

[enter details]

4. Certification by directors [if not director, replace with appropriate equivalent]

[Grantee name]

[Project number]

For the period [dd/ mm/yyyy] to [dd/ mm/yyyy]

We confirm that, to the best of our knowledge and believe, having made such enquiries as we considered necessary for the purpose of appropriately informing ourselves:

Statement of grant income and expenditure

a. We have fulfilled our responsibilities for the preparation of the statement of grant income and expenditure in accordance with the cash basis of accounting and the terms of the grant agreement with the Commonwealth, represented by the Department of Industry, Science and Resources dated [enter date]; in particular, the statement of grant income and expenditure presents fairly in accordance therewith.

b. All events subsequent to the date of the statement of grant income and expenditure which require adjustment or disclosure so as to present fairly the statement of grant income and expenditure, have been adjusted or disclosed.

c. [Where applicable] The effects of uncorrected misstatements are immaterial, both individually and in the aggregate, to the statement of grant income and expenditure as a whole. A list of the uncorrected misstatements is attached to this representation letter.

d. That all Grantee contributions and other financial assistance were spent for the purpose of the project and in accordance with the grant agreement and that the Grantee has complied with the grant agreement and relevant accounting policies.

e. That salaries and allowances paid to persons involved in the project are in accordance with any applicable award or agreement in force under any relevant law on industrial or workplace relations.

Signature .....

Name [enter name]

Director

Date [dd/mm/yyyy]

Signature .....

Name [enter name]

Director

Date [dd/mm/yyyy]

5. For Auditor use only

I certify that this statement of grant income and expenditure is the one used to prepare my independent audit report dated [enter date] for the Department of Industry, Science and Resources.

Signature .....

Name	[enter name]
Position	[enter position]
Auditor's employer	[enter employer name]
Date	[dd/mm/yyyy]

Attachment B - Independent audit report

Background for auditors

The purpose of the independent audit report is to provide us with an auditor's opinion on the Grantee's statement of grant income and expenditure. The statement of grant income and expenditure is prepared by the Grantee to correspond with the expenditure reported to the department by the Grantee for the same period, in the process of claiming grant payments.

The independent audit report must be prepared by a person who is an approved auditor.

An approved auditor is a person who is:

a. registered as a company auditor under the *Corporations Act 2001* or an appropriately qualified member of Chartered Accountants Australia and New Zealand, or of CPA Australia or the Institute of Public Accountants; and

b. not a principal, member, shareholder, officer, agent, subcontractor or employee of the Grantee or of a related body corporate or a Connected Entity.

The audit should be undertaken and reported in accordance with Australian Auditing Standards.

The independent audit report must follow the required format and include any qualification regarding the matters on which the auditor provides an opinion. We may follow up any qualifications with the Grantee or auditor. The independent audit report must be submitted on the auditor's letterhead.

Auditors must comply with the professional requirements of Chartered Accountants Australia and New Zealand, CPA Australia and the Institute of Public Accountants in the conduct of their audit.

If the auditor forms an opinion that the statement of grant income and expenditure does not give a true and fair view of the eligible expenditure for the period, the independent audit report should be qualified and the error quantified in the qualification section of the independent audit report.

The required independent audit report format follows.

Auditor's report

Independent audit report in relation to [Grantee name]'s statement of grant income and expenditure to the Commonwealth, represented by the Department of Industry, Science and Resources (the department).

We have audited:

a. the accompanying statement of grant income and expenditure of [Grantee name] for the period [dd/mm/yyyy] to [dd/mm/yyyy], a summary of significant accounting policies and other explanatory information, and management's attestation statement thereon (together "the financial statement"). The financial statement has been prepared by management using the cash basis of accounting described in note 3.2 to the financial statement; and

b. [Grantee name]'s compliance with the terms of the grant agreement between [Grantee name] and the Commonwealth dated [date of agreement] for the period [dd/mm/yyyy] to [dd/mm/yyyy] (the grant agreement).

We have:

a. reviewed [Grantee name]'s statement of labour costs in support of its claim of eligible expenditure[; and

b. performed limited assurance procedures on [Grantee name]'s statement of employee numbers under the grant agreement].

Management's responsibility

Management is responsible for:

a. the preparation and fair presentation of the financial statement in accordance with the basis of accounting described in note 3.2, this includes determining that the cash basis of accounting is an acceptable basis for the preparation of the financial statement in accordance with the grant agreement;

b. compliance with the terms of the grant agreement;

c. the preparation of the statement of employee numbers and labour costs in support of eligible expenditure; and

d. such internal control as management determines is necessary to:

    i enable the preparation of the financial statement and the statement of [employee numbers and] labour costs that are free from material misstatement, whether due to fraud or error; and

    ii enable compliance with the terms of the grant agreement.

Auditor's responsibility

Our responsibilities are:

a. To express an opinion, based on our audit, on:

    i the financial statement; and

    ii [Grantee name]'s compliance, in all material respects, with the terms of the grant agreement; and

b. To conclude based on:

   i our review procedures, on the statement of labour costs; and

   ii our limited assurance procedures on the statement of employee numbers.

We conducted our audit of the financial statement in accordance with Australian Auditing Standards; our audit of compliance with the grant agreement in accordance with ASAE 3100, our review of the statement of labour costs in accordance with ASRE 2405[; and our limited assurance procedures on employee numbers in accordance with ASAE 3000]. The applicable Standards require that we comply with relevant ethical requirements and plan and perform our work to:

a. obtain reasonable assurance about whether the financial statement is free from material misstatement and that [Grantee name] has complied, in all material respects, with the terms of the grant agreement; and

b. obtain limited assurance as to whether anything has come to our attention that causes us to believe that the statements of employee numbers and labour costs are materially misstated.

An audit involves performing procedures to obtain audit evidence about the amounts and disclosures in the financial statement and about the Grantee's compliance with the grant agreement. The procedures selected depend on the auditor's judgement, including the assessment of the risks of material misstatement of the financial statement, whether due to fraud or error. In making those risk assessments, the auditor considers internal control relevant to the Grantee's preparation and fair presentation of the financial statement, and to the Grantee's compliance with the grant agreement, in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the Grantee's internal control. An audit also includes evaluating the appropriateness of accounting policies used by management, as well as evaluating the overall presentation of the financial statement.

A review consists of making enquiries and applying analytical and other review procedures. A review is substantially less in scope than an audit conducted in accordance with Auditing Standards and consequently does not enable us to obtain assurance that we would become aware of all significant matters that might be identified in an audit. Accordingly, we do not express an audit opinion on the statement of labour costs.

A limited assurance engagement undertaken in respect of the statement of employee numbers, in accordance with ASAE 3000 involves [level of detail about procedures to be determined by the auditor]. The procedures performed in a limited assurance engagement vary in nature and timing from, and are less in extent than for, a reasonable assurance engagement; and consequently, the level of assurance obtained in a limited assurance engagement is substantially lower than the assurance that would have been obtained had a reasonable assurance engagement been performed.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our audit opinion, review and limited assurance conclusions.

Opinion

In our opinion:

a. the financial statement presents fairly, in all material respects, the grant income and expenditure of [Grantee name] for the period [dd/mm/yyyy] to [dd/mm/yyyy] in accordance with the cash basis of accounting described in note 3.2 and the terms of the grant agreement, dated [date of agreement], with the Commonwealth; and

b. [Grantee name] has complied, in all material respects, with the requirements of the grant agreement between the organisation and the Commonwealth dated [date of agreement], for the period [dd/mm/yyyy] to [dd/mm/yyyy].

Basis of Accounting and Restriction on Distribution

Without modifying our opinion, we draw attention to note 3.2 to the financial statement, which describes the basis of accounting. The financial statement is prepared to provide information to the department in accordance with the grant agreement, dated [date of agreement]. As a result, the financial statement may not be suitable for another purpose.

Use of Report

This report has been prepared for [Grantee name] and the department in accordance with the requirements of the grant agreement between [Grantee name] and the Commonwealth, dated [date of agreement]. We disclaim any assumption of responsibility for any reliance on this report to any persons or users other than [Grantee name] and the department, or for any purpose other than that for which it was prepared.

Conclusions

Based on:

a. Our review, which is not an audit, nothing has come to our attention that causes us to believe that the statement of labour costs in the period [dd/mm/yyyy] to [dd/mm/yyyy] is not, in all material respects, fairly presented in accordance with the grant agreement dated [date of agreement] with the Commonwealth[; and

b. The procedures we have performed and the evidence we have obtained, nothing has come to our attention that causes us to believe that the statement of employee numbers as at [dd/mm/yyyy] is not prepared, in all material respects, in accordance with the grant agreement dated [date of agreement] with the Commonwealth].

Auditor's signature	.....
Name	[enter name]
Auditor's employer	[enter employer name]
Employer's address	[enter address]
Qualifications	[enter qualification]
Position	[enter position]
Date	[dd/mm/yyyy]

Attachment C - Certification of certain matters by the auditor

The department also requires a certification of certain matters by the auditor in addition to the independent audit report. This should be submitted with the statement of grant income and expenditure and independent audit report.

The auditor who signs this certification must also initial and date a copy of the Grantee's statement of eligible expenditure. The department will not accept an independent audit report that lacks this attachment.

The required format of certification is on the following page.

[print on auditor letterhead]

[addressee]
Department of Industry, Science and Resources
GPO Box 2013
Canberra ACT 2601

I understand that the Commonwealth, represented by the Department of Industry, Science and Resources and [Grantee name] have entered into a grant agreement for the provision of financial assistance under the [grant opportunity name] to the Grantee for the project. A condition of funding under the grant agreement is that the Grantee provides a statement of grant income and expenditure certifying that expenditure on approved project items has been incurred within the relevant audit period and paid in accordance with the grant opportunity guidelines, and is supportable by appropriate documentation.

In fulfilment of the condition, I hereby certify that:

a. I am a member of Chartered Accountants Australia and New Zealand/ CPA Australia/ the Institute of Public Accountants (as a Public Practice Certified Member).

b. I have prepared the independent audit report on [Grantee name]'s, statement of grant income and expenditure in accordance with the details of the grant agreement between the Grantee and the Commonwealth, project no [project no] dated [dd/mm/yyyy].

c. I have reviewed the grant agreement between the Grantee and the Commonwealth, project no [project no] dated [dd/mm/yyyy], and related grant opportunity guidelines and understand the requirements pertaining to financial reporting and eligible expenditure contained therein.

d. I have signed the attached copy of [Grantee name]'s statement of eligible expenditure that I used to prepare the independent audit report.

e. I have complied with the professional independence requirements of Chartered Accountants Australia and New Zealand/ CPA Australia/the Institute of Public Accountants. I specifically certify that I:

    i am not, and have not been, a director, office holder, or employee of [Grantee name] or related body corporate of [Grantee name]

    ii have not been previously engaged by [Grantee name] for the purpose of preparing their [grant opportunity name] application or any report required under the grant agreement

    iii have no financial interest in [Grantee name].

Signature .....

Name [enter name]

Qualifications [enter qualification]

Position [enter position]

Date [dd/mm/yyyy]

Australian Government
Department of Industry, Science and Resources

Deed of Variation

Small Business Cyber Wardens

SBCW000001

Details

Parties

The parties to this deed of variation including any schedules and annexures ("Deed") are the parties to the grant agreement with number SBCW000001 executed on 6/11/2023 under Small Business Cyber Wardens as varied from time to time ("Grant Agreement").

Definition

Unless otherwise specified or the context otherwise requires, terms that are defined in the Grant Agreement have the same meaning in this Deed.

Background

The Commonwealth and the Grantee have agreed to vary the terms of the Grant Agreement in accordance with this Deed.

Operative clauses

1. On and with effect from 10 February 2025, the Grant Agreement is varied as set out in Schedule 1 to this Deed.
2. The parties confirm all other provisions of the Grant Agreement and, subject only to the amendments contained in this Deed, the Grant Agreement remains in full force and effect.
3. This Deed and the Grant Agreement, when read together, contain the entire agreement of the parties with respect to the parties' rights and obligations under the Grant Agreement.
4. This Deed may be executed in any number of counterparts. All counterparts, taken together, constitute one instrument. A party may execute this Deed by signing any counterpart.
5. This Deed is governed by the laws of the Australian Capital Territory.
6. Each party will pay their own costs associated with this Deed.

Signatures

Executed as a deed:

Commonwealth

Executed as a deed for and on behalf of the Commonwealth of Australia as represented by the Department of Industry, Science and Resources by:

Name (print)	s 47F
Position (print)	STATE MANAGER SA/WA
Signature and date	s 47F 19/2/2025
Witness name (print)	s 47F
Signature and date	s 47F 19/2/2025

Grantee

Executed as a deed for and on behalf of COUNCIL OF SMALL BUSINESS ORGANISATIONS OF AUSTRALIA LIMITED in accordance with section 127 of the *Corporations Act 2001* by:

Name of company	COUNCIL OF SMALL BUSINESS ORGANISATIONS OF AUSTRALIA LIMITED ABN 43008597304 ACN 008597304
Director name (print)	s 47F
Signature and date	18/02/2025
Director/ Company Secretary name (print)	
Signature and date	18/02/2025

Schedule 1 - Variation to Grant Agreement

1. The Grant Details are varied

a. Clause B is varied by deleting the Project scope and description and replacing it with the following:

The program's final milestones, deliverables, and budget will be agreed between COSBOA and the Department in an updated Project Plan provided in Milestone 3 to ensure alignment with the government's Cyber Strategy.

Full details of program activities, including breakdown of program deliverables, are included in the attached Project Plan.

Indicative activities:
Workstream #1: Research and evidence
#1.1 Annual 'Small Business Cyber Security Pulse Check' report
Research whitepaper providing 'state of the nation's small business and cyber security benchmarking, with a focus on measuring behavioural change and tracking emerging needs of Australian small business owners.
#1.2 National small business cyber security survey on preparedness and capability of small business owners and teams. Survey to be repeated annually over the life of the grant.
#1.3 Qualitative research
Focus groups and in-depth interviews across a range of small business sizes and demographic segments (including sole traders, micro SBs, mid-sized SBs, rural businesses, as well as founders who identify as female, culturally and linguistically diverse, Aboriginal and Torres Strait Islander and founders with a disability.)
#1.4 Communication and distribution strategy inclusive of annual industry research briefings and webinar, national media research launch and associated media support.

Workstream #2: Industry consultation and co-design
#2.1 General program consultation
Consultation and codesign activities to inform national Cyber Wardens program development.
Building on Level 1, developed through the pilot program, Cyber Wardens Levels 2 and 3 will be implemented in Year 1, with 3x Industry / Sector specific extensions in Year 2.
#2.2 Program Translation Consultation
Co-design and consultation with diverse audience segments.
#2.3 Program Expansion Report
Co-design and consultation recommendations and report synthesising insights and recommendations from codesign activities.
#2.4 Small Business Cyber Security 5 Year Strategy
Design of 5 Year Small Business Cyber Security Strategy with Cyber Wardens program recommendations.

Workstream #3: Program & platform development
#3.1 Educational design
Design of the educational outcomes and learning framework to guide the development of individual course components.
#3.2 E-learning modules and content development
End-to-end content and module development for the Cyber Wardens platform comprising

wireframes, content creation, user testing and ongoing content maintenance

#3.3 Facilitated learning development

Development of content resources to support in-person learning, immersion workshops and facilitated sessions.

#3.4 Small business Cyber Wardens Resources Hub

Practical small business resources

#3.5 Brand

Cyber Wardens brand review and refinement.

#3.6 Platform hosting and management

Technical development, platform upgrades, maintenance, hosting, management.

#3.7 Cyber security

Security stress-testing of platforms and insurance

Workstream #4: National awareness and education campaign

#4.1 National awareness and education campaign

33-month awareness and education plan, with annual review and update to identify emerging opportunities and integrate them into the communication strategy.

#4.2 Media

National and industry media events and PR, alongside ongoing social media

#4.3 Stakeholder engagement

Ongoing engagement with small business peak body organisations

#4.4 Awareness content and activities

Ambassadors program, Local Electorate Cyber Wardens Kits, podcast, and major video campaign.

#4.5 Paid amplification

Paid advertising and media.

Workstream #5: Student recruitment and behavioural change

#5.1 Recruitment

Targeted and tailored recruitment activities for new learners, recertification and future modules

#5.2 Student support

Design and delivery of communications to students

#5.3 Graduation

Development, manufacture and fulfilment of graduation kit and recertification materials

#5.4 Driving behavioural change

Implementation program

Workstream #6: Reporting and evaluation

#6.1 Project Reporting

Grant reporting

#6.2 Evaluation

Design of student evaluation framework, survey creation and testing, market research approvals, collection and reporting

Workstream #7: Project management

#7.1 Work plan

Design of the 3-year program implementation work plan

#7.2 Advisory Group Management

Quarterly meetings of the Cyber Wardens Industry Advisory Group

#7.3 Project & Grant Management

Including financial and operations oversight of project sourcing, management of contractors, and so on

b. Clause B is varied by deleting the Project outcomes and replacing it with the following:

A 3-year investment from the Australian Government would deliver Australia's first small business cyber security frontline comprised of employees and owners from the nation's 2.3 million small businesses. This investment would supercharge behavioural change in homes and businesses across Australia - with safer online practices closing Australia to the business of cyber criminals.

Rolling out the Cyber Wardens program nationally will:
1. Empower small businesses to help protect themselves against cyber threats by training up to 60,000 Cyber Wardens across at least 15,000 small businesses with free access to the Cyber Wardens eLearning program.

2. Increase small business awareness of cyber security threats and awareness of readily available solutions to build their cyber resilience by engaging with more than 1 million small business owners and employees through a high-impact national awareness campaign.

3. Build a network of trained in-house cyber wardens to drive cultural change and cyber-safe mindsets in Australia's small business.

4. Develop the practical skills of small businesses to guard against cyber security threats.

5. Provide a Rapid Response Platform for small business to respond quickly to emerging cyber threats with targeted information and resources.

6. National program footprint including 24 Cyber Wardens roadshow events and the supply of local Cyber Wardens kits.

Nearly half of all Australians employed in small businesses have experienced a negative cyber incident. If just 20 per cent of businesses trained by Cyber Wardens could successfully detect and thwart a cyberattack, the financial gain for the industry could amount to $117 million. This equates to a potential ROI of at least 4x.

In undertaking the Activity, the Grantee must comply with the requirements of the grant opportunity guidelines (as in force at the time of application).

The Grantee must notify the Commonwealth about events relating to the project and provide an opportunity for the Minister or their representative to attend.

c. Clause C is varied by deleting the Activity Schedule and replacing it with the following:

Milestone number	Milestone name and description	Due date
001	Milestone 1: Project Launch & Design Risk Register and Mitigation Plan design Program Launch Evaluation design Inaugural Small Business Cyber Security Research Project and associated media and research webinar Program Learning Framework and strategy design Pilot content review Launch ambassador program Student recruitment, graduation and support services Project Management Resource Hub launch Content production National awareness & education campaign Measurable Targets: - By the end of this milestone period, it is expected that the Cyber Wardens project will have cumulatively achieved the following targets: - Enrolments 1,000 - Graduates 500 - Small businesses engaged 150 Any of these measurable targets not achieved by the end of this milestone period will be expected to be made up in future milestone periods. The grantee is required to supply additional budget evidence in their first progress report as follows: - The grantee supplies further evidence to labour costs by specifying the funded positions inclusive of Part-Time/Full-Time Equivalent (PTE/FTE) staffing and the number of staff associated with direct labour costs. - The grantee supplies further evidence to travel expenditure such as class of travel, duration, accommodation, and number of travellers.	29/02/2024

Milestone number	Milestone name and description	Due date
002	Milestone 2: Facilitated Learning Design & Consultation Podcast development and launch Student recruitment, graduation and support services Project Management Resource Hub management Content production National awareness & education campaign Measurable Targets: - By the end of this milestone period, it is expected that the Cyber Wardens project will have cumulatively achieved the following targets: - Enrolments: 7,500 - Graduates: 6,000 - Unique small businesses engaged: 1,800 Any of these measurable targets not achieved by the end of this milestone period will be expected to be made up in future milestone periods.	31/07/2024

Milestone number	Milestone name and description	Due date
003	Milestone 3: Program Extension Project Plan with detailed milestones and deliverables confirmed. Local Activations Kit and Local Electorate Pop-Ups Program Extension Consultation across program levels, audience translations and industries. Annual Recertification strategy, wireframes, content creation, user testing and platform development Program Extension: Emerging threat module development (if required). Recertification platform production Level 2 & 3 design and content production Train the Advisor final production and launch Program extensions: Emerging Threat module development and Lunch & Learn Kits Annual Small Business Cyber Security Research Project and associated media Student recruitment, graduation and support services Project management Resource Hub management Content production National awareness & education campaign Measurable Targets: - By the end of this milestone period, it is expected that the Cyber Wardens project will have cumulatively achieved the following targets: - Enrolments: 17,000 - Graduates: 14,300 - Recertifications: 1,500 - Unique small businesses engaged: 4,290 Any of these measurable targets not achieved by the end of this milestone period will be expected to be made up in future milestone periods.	31/01/2025

Milestone number	Milestone name and description	Due date
004	Milestone 4: Mid project impact and program amplification Train the Advisor & facilitate learning strategy, content and resource development. Mid-project impact report Level 2 & 3 Launch Program Extension: Emerging threat module user testing & sector extension development Program adaptations: Final production for train the advisor Program adaptations: CALD translations and target audience - tailored content CALD & Aboriginal and Torres Strait Islander targeted content Development and launch of podcast season 2 Student recruitment, graduation and support services Project management Resource Hub management Content production National Awareness & education campaign Measurable Targets: - By the end of this milestone period, it is expected that the Cyber Wardens project will have cumulatively achieved the following targets: - Enrolments: 29,000 - Graduates: 25,000 - Recertifications: 6,000 - Unique small businesses engaged: 7,500 Any of these measurable targets not achieved by the end of this milestone period will be expected to be made up in future milestone periods.	31/07/2025

Milestone number	Milestone name and description	Due date
005	Milestone 5: Program amplification Ongoing project delivery Program Adaptations: CALD translations Annual Small Business Cyber Security Research Project and associated media Program Extension: Emerging threat module Annual Content Review Student recruitment, graduation and support services Project management Resource Hub management Content production National Awareness & education campaign Measurable Targets: - By the end of this milestone period, it is expected that the Cyber Wardens project will have cumulatively achieved the following targets: - Enrolments: 45,000 - Graduates: 38,000 - Recertifications: 13,500 - Unique small businesses engaged: 11,400 Any of these measurable targets not achieved by the end of this milestone period will be expected to be made up in future milestone periods.	31/01/2026

Milestone number	Milestone name and description	Due date
006	Milestone 6: Amplification + evaluation Ongoing project delivery Project Evaluation National Awareness & education campaign inclusive off media + trade media campaign, 3 webinars, 3 trade booth, quarterly ambassador, branded content partnership Paid amplification 250K + 1250K search Project Management Resource Hub management Content production National Awareness & education campaign Measurable Targets: - By the end of this milestone period, it is expected that the Cyber Wardens project will have cumulatively achieved the following targets: - Enrolments: 60,000 - Graduates: 50,000 - Recertifications: 24,000 - Unique small businesses engaged: 15,000 As this is the final milestone, it is expected that these targets will be fully achieved.	31/07/2026

d. Clause F is varied by deleting the Commonwealth representative and address section and replacing it with the following:

Name of representative	s 47F
Position	Program Manager - Business Grants Hub
Postal address	GPO Box 2013 CANBERRA ACT 2601
Physical address	10 Binara Street CANBERRA ACT 2600
Business hours telephone	s 47F
Email	CyberWardens@industry.gov.au

The Parties' representatives will be responsible for liaison and the day-to-day management of the Grant, as well as accepting and issuing any written notices in relation to the Grant.

2. The Supplementary Terms are varied

a. Subclause ST2.2 is varied by deleting the subclause and replacing it with the following:

The Grantee agrees to use the Grant and any Other Contributions and undertake the Activity consistently with the Activity Budget in the following table:

Financial Year 2023/24

Head of expenditure	Breakdown of expenditure	Agreed project cost
Project expenditure	s 47(1)(b)	
Project expenditure		
Project expenditure		
Project expenditure		
Project expenditure		
Project expenditure		
Project expenditure		
Project expenditure		
Project expenditure		
Financial year total		$6,589,535

Financial Year 2024/25

Head of expenditure	Breakdown of expenditure	Agreed project cost
Project expenditure	s 47(1)(b)	
Project expenditure		
Project expenditure		
Project expenditure		
Project expenditure		
Project expenditure		
Project expenditure		
Project expenditure		
Project expenditure		

Financial year total	$8,401,088

Financial Year 2025/26

Head of expenditure	Breakdown of expenditure	Agreed project cost
Project expenditure	s 47(1)(b)	
Project expenditure		
Project expenditure		
Project expenditure		
Project expenditure		
Project expenditure		
Project expenditure		
Project expenditure		
Project expenditure		
Financial year total		$8,004,127

Financial Year 2026/27

Head of expenditure	Breakdown of expenditure	Agreed project cost
Project expenditure	s 47(1)(b)	
Project expenditure		
Project expenditure		
Project expenditure		
Project expenditure		
Project expenditure		
Project expenditure		
Project expenditure		
Project expenditure		
Financial year total		$0

All financial years

Head of expenditure	Breakdown of expenditure	Agreed project cost
Project expenditure	s 47(1)(b)	
Project expenditure		
Project expenditure		
Project expenditure		
Project expenditure		
Project expenditure		
Project expenditure		
Project expenditure		
Project expenditure		
All financial years total		$22,994,750

Figures in the above table are GST inclusive amounts less GST credits that can be claimed in relation to the expenditure.

Cyber Wardens program

Midpoint Evaluation Report

July 2025

Citation: First Person Consulting (2025). Midpoint Evaluation of the Cyber Wardens program. Prepared for 89 Degrees East, Melbourne, Victoria.

Executive Summary

The Cyber Wardens program is an initiative of the Council of Small Business Organisations Australia (COSBOA), funded by the Australian Government and supported by an industry alliance led by Telstra, CommBank and the Australian Cyber Security Centre. Delivered by 89 Degrees East, at its core, Cyber Wardens is about improving the resilience of small businesses by improving their cyber security posture and capabilities.

Broadly, there are three core components – an awareness raising effort (e.g. social media), a resource hub, and the Cyber Wardens training modules. Through completion of the Foundations and Course Level 1 training modules, businesses will have capable staff ('Cyber Wardens') that will support their cyber security needs. Subsequent courses (i.e. Level 2, Level 3) and other mechanisms will extend learning and help maintain relevance with emerging trends and threats.

In simple terms, Cyber Wardens will be the online version of first aid officers or fire safety wardens, who can prevent, prepare, fight and help recover from a cyber attack or the theft of customer data or intellectual property.

First Person Consulting has been engaged as the independent evaluator of the Cyber Wardens program. This evaluation report analyses recent data collected – including from Level 2 training and new Level 1 training participants. It builds off the initial evaluation that we completed in late 2024.

Findings from the midpoint evaluation survey data are highly positive. With sufficient responses to suggest confidence in generalising findings, we can say that:

- Through participation in the Cyber Wardens training, **participants increase their understanding of the cyber security risks that face small businesses, what cyber security means to a small business, and the ways cyber security can increase.**
- **Most participants either intend to take an action as a result of the course or are already doing that action** to increase Cyber-Security.
- **There are opportunities to strengthen the ongoing engagement with course participants**, as survey respondents were not highly engaged with the Resource Hub, or aware of Cyber-Wardens alerts.

In terms of demonstrated outcomes, the program continues to make good progress off the back of what was demonstrated in the initial evaluation. There are some considerations based on the survey data of where effort could be invested to strengthen the program. These are noted later in the report.

Introduction

Background

Research tells us that risk to small businesses from cyber-attacks and crime is substantial. Small businesses cannot rely on their size to 'hide' from these risks. At its core, Cyber Wardens is about improving the resilience of small businesses. It is free, online, and centred on making small businesses cyber-safe through a series of short modules and other resources.

The Cyber Wardens program is an initiative of the Council of Small Business Organisations Australia (COSBOA), funded by the Australian Government and supported by an industry alliance led by Telstra, CommBank and the Australian Cyber Security Centre. Cyber Wardens complete online training and then working within the business to help prevent, prepare, fight and recover from a cyber attack or the theft of customer data or intellectual property

The goals of the Cyber Wardens program are to:

- Attract 60,000 enrollees by 31 July 2026
- Convert 50,000 enrollees to graduates by 31 July 2026
- Engage more than 15,000 small businesses by 31 July 2026
- Have 24,000 graduates recertify through the life of the program

You can find out more about the Cyber Wardens program on their website.

First Person Consulting (FPC) was engaged in mid-2024 to design and implement an independent evaluation of the Cyber Wardens program. This midpoint evaluation report builds on the initial evaluation completed in late 2024 and outlines the approach to the final evaluation due in 2026.

Evaluation objectives

This independent evaluation of the Cyber Wardens program will gather evidence on the activities, achievements, opportunities and challenges over the course of the program.

The objectives of the evaluation are to:

- Determine the extent to which grant deliverables are successfully completed or produced
- Determine the extent to which intended outcomes for small business owners / sole traders, small business employees, and the business itself are achieved
- Gathers learning from participants, industry partners, and COSBOA members on the program
- Determines the actual, likely, and/or potential economic benefits of trained Cyber Wardens.

It is important to recognise that there are three types of targeted participant in the Cyber Warden's program: small business owners/small traders, small business employees, and the entity. Where the term 'participant' is used it is a general reference to these three groups, unless otherwise specified.

The evaluation draws on a range of data sources and inputs and will result in a series of deliverables. To date, an **internal-facing evaluation plan** and **an initial evaluation report** have already been produced.

The relevant components of the **evaluation plan** – being the program logic model, the Key Evaluation Questions (KEQs), and indicators – are summarised in this report.

The initial evaluation report summarised the key data points for the Cyber Wardens program and provided recommended changes to data collection to support the evaluation.

This report constitutes the third deliverable of four – **a midpoint evaluation report that builds off the initial evaluation report.** A **final evaluation report** will be produced in July 2026, which will present the final results of the evaluation, and address the objectives of the evaluation.

Midpoint Evaluation

Key Evaluation Questions and Program Logic Model

The table below contains the evaluation questions used to guide this report. Three sub-questions (marked with '*') relate to the economic evaluation that will be produced in the final report. With the data provided to this date, we will briefly outline how these questions will be addressed and the data that will be required. The program logic model which outlines the outputs and outcomes for the Cyber Wardens program is provided over the page.

Key Evaluation Questions	Sub-questions	Things to look for (indicators / measures)
Delivery **1. To what extent is the design of and approach to the Cyber Wardens program appropriate?**	a) What has the recruitment and retention approaches for the Program looked like? b) What activities have been delivered through the Cyber Wardens program so far? c) What have been the main outputs resulting from the Cyber Wardens program? d) How cost-effective was the Cyber Wardens program since commencement?*	• Marketing approaches and data (e.g. social media analytics) • Delivery information and data for events and engagement • # of enrolments / # of graduations • # of attendees at webinars / other events • Cost-Effectiveness Analysis ($ per output)*
Outcomes **2. To what extent is the Cyber Wardens Program working as intended?**	a) What is the evidence for the outcomes occurring as per the logic model? b) What evidence is there for any unintended outcomes (positive or negative?) c) What are the economic benefits of the Cyber Wardens program?*	• Retention rates / engagement rates throughout the program • Proportion of attendees demonstrating improved outcomes • Net Promoter Score • Qualitative feedback indicating a good user journey / benefits from the program • Evidence of any other outcomes • Cost-Benefit Analysis and Cost-Avoidance Analysis*
Learning **3. What learning has resulted so far?**	a) What is the Cyber Wardens program doing well? b) What opportunities to change or strengthen the program are there?	• Interpretation of collected data • Feedback from users • Interviews with the program team

Problem/need statement: Cyber security is an identified national security problem: threats are more frequent, sophisticated and costly for Australian businesses (avg of $46,000 for each attack). Small businesses currently lack the skills and resources necessary to ensure cyber security and need fit-for-purpose solutions with simple language focused on incremental improvements.

Program objective: To enhance small business cyber resilience by empowering 60,000 Cyber Wardens in 15,000 small businesses across Australia by 2026 through a national awareness and education campaign, and targeted, accessible and simplified training focused on behavioral change delivered via a free and easy to use e-learning platform.

Inputs

- **Evidence-based research to inform program design**
- **Partnerships and consultation:**
- **Federal Government Cyber Security Strategy**
- **Funding**

Activities

- **Learning Program:** Cyber Wardens design and deliver a cyber security education program through eLearning platforms
- **Cyber Wardens Resource Hub**: An online resource hub offering engaging and specialty content
- **Cyber Security Awareness & Education Campaign:** A national education campaign targeting small businesses through inspiring content, community engagement and local activation

Outputs

- **Student recruitment has occurred**
  - Number of enrolments, graduates and recertifications
  - Number of SME's engaged
  - Customer support
- **eLearning and behaviour change programming delivered**
  - Number of modules
  - Tailored content and translations
  - Behaviour change program
- **Resource Hub:**
  - Number of resources
  - Reach and engagement with resources and the resource hub
- **Awareness campaigns implemented**
  - Number/reach of ambassadors
  - Number of local electoral/training resources
  - Number/reach of podcasts
  - Number of media campaigns and activities
  - Reach and engagement of social media
- **Stakeholder engagement undertaken**
  - Number and type of engagements with trade and industry activities

Short-term outcomes

- Graduates have increased knowledge of basic cyber safety hygiene, spotting and addressing threats
- Graduates have increased confidence to implement stronger cyber security posture
- Graduates elect to enroll in additional modules and course extensions
- Businesses can easily access tools and resources that are fit for purpose
- Users are informed about threats and methods to increase cyber security posture
- Increased awareness of the importance of cyber security among SMEs
- SME/businesses recognize the need to address Cyber Security posture and are aware of opportunities to do so

Medium-term outcomes

- Graduates have basic technical knowledge to address and prevent common threats
- Graduates have increased confidence to take on in-house cyber safety officer roles
- SME's see cyber security as an important internal capability
- There is demonstrable improvement in cyber security posture among SMEs with employed Cyber Warden program graduates
- SMEs are empowered to engage with the Resource Hub as a source to revisit and update knowledge and skills
- The Resource Hub is embedded into SME operations and processes as a key source of cybersecurity knowledge
- Increase in course enrolment and graduates due to improved cyber awareness among SMEs

End of program outcomes

- SMEs exhibit a strong proactive cyber posture and with tested response, recovery and continuity processes following engagement with the program
- Cultural leadership of cyber safety is practiced at the business.
- SMEs who engage with the program allocate more funding and resources to cyber security practices and platforms
- The Resource Hub contributes to training, knowledge-sharing and collaboration among SMEs to enhance collective knowledge
- Overall increase in cyber security knowledge of general team due to engagement with their Cyber Wardens graduates and the Resource Hub
- There are more SMEs and employees practicing and aware of safe cyber security practices
- Annual recertification and updating of cyber posture by SMEs in response to new and emerging threats

Wider goals

- Australian SMEs are empowered to uplift cyber security because of improved staff capabilities
- Australian SMEs are better equipped to prevent, mitigate and manage cyber security incidents
- Australian SMEs avoid costs associated with incidents because of their increased cyber security capabilities

Key

- Participation
- Resource Hub
- Marketing

Approach to this report

To commence the evaluation, a **robust planning stage was undertaken.** The purpose of this process was to:

1. Set clear objectives for the evaluation to ensure that we had a clear understanding of the needs of all parties involved
2. Develop our understanding of the background to the Cyber Wardens program, including the different components associated with delivery
3. Review the current data collection processes and identify the feasibility for incorporating new processes.

Following this process, we developed a **program logic model and evaluation approach.** This was tested and refined with 89 Degrees East to ensure that it aligned with their objectives and plans for delivery.

Following the development of the plan, an **initial evaluation was undertaken.** This provided a chance to sense-check the feasibility of intended outcomes and identify ways to enhance longer-term data collection.

This report marks the third key deliverable, with the final evaluation due mid-

The **inputs** into this midpoint report are summarised below. These include reports, primary survey data collected from participants in the Cyber Warden program. Sample sizes are noted where relevant.

Information was analysed in alignment with the KEQs on the previous page. We used a mixture of thematic analysis for qualitative data, and descriptive analysis for quantitative data. Content analysis from desktop review of reports has been used to supplement questions with specific sources referenced.

Documents and information reviewed included:

- 2025 Cyber Wardens Advisory Board Report
- Impact and Action Survey - Foundations and Course Level 1 (Manual and Automated) and Course Level 2 (Manual and Automated) (Combined Impact and Action survey n=175)
- Graduation Survey – Course Level 1 (n=72) and Course Level 2 (n=188)
- Cyber Wardens course catalogue and contribution to KPIs
- Cyber Wardens Treasury Approved Data
- Cyber Wardens Data submitted for Treasury assessment
- COSBOA Member Report
- Eligible Engaged Small Businesses
- All recertifications report
- Eligible recertifications report
- Value add participants
- Owner or employee participant report

Report structure

The report covers the following:

1. Findings against the guiding evaluation questions for the midpoint evaluation:
    a) Covering participation data collected since the launch of the Cyber Wardens program to 30 June 2025.
    b) Analysis of survey data collected from participants who completed of the Level 1 and Level 2 courses, and follow-up survey data to understand evidence of behaviour change
    c) A summary of learning based on survey comments.
2. An overview of the economic evaluation approach, data requirements, and how this will inform the final evaluation report.
3. Recommendations based on the results presented in this report.

We note that the level of survey data is lower than anticipated. There was a survey from a different provider distributed to participants in May / June 2025, which may have influenced response rates to the tools used in this evaluation.

That said, the results in this report should also be viewed in conjunction with the positive findings from the initial evaluation. A summary of these has also been included for ease of review.

Findings – Program Delivery

Program design

Since the initial evaluation report the number of offerings have continued to increase. The approach for the Cyber Wardens core program – summarised in the Figure to the right – reflects a common model for learning (beginner through to advanced).

The Foundations Course, Course Level 1 and Course Level 2 are live, and Course Level 3 launched August 4. The 'Train-the-Trainer' course will launch 25 August, and the 'emerging threats' offering is delivered on an 'as needed' basis.

In the initial evaluation we only had early data largely reflective of experiential feedback (e.g. satisfaction with content) and immediate learning outcome from Course Level 1.

Since that time, it is clear that the Cyber Wardens offering has evolved significantly – as is reflected in the summary to the right and as discussed in the June 2025 Cyber Wardens Advisory Board Meeting slide deck report. In particular, we note that there is ongoing efforts to continuously improve existing content (e.g. from a user experience perspective), as well as the development of new content.

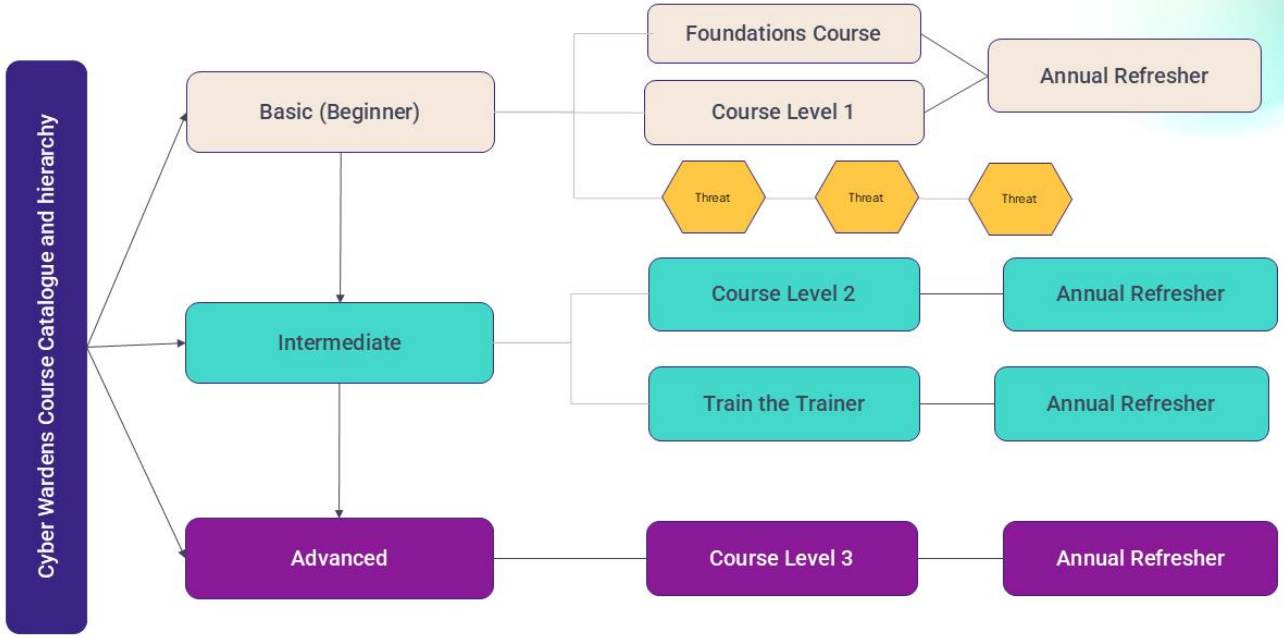


*Figure: Breakdown of Cyber Wardens course offerings.**

* Source: Taken from the 'Cyber Wardens course catalogue and course contribution to KPIs' PPTX file provided by 89 Degrees East.

Program delivery

Information on the outputs from the Cyber Wardens Program to date have been taken from documentation provided.

Promotion of the Cyber Wardens program occurs through a variety of channels and partnerships. The detail of these is described in the June 2025 Advisory Board Report Deck, but the key figures that stand out include:

- "Strong national media reach, with 360 total media mentions and an estimated potential audience reach of 2.86 million people." (pg. 28)
- 99 webinars and dozens of relationships with sector groups to drive awareness raising
- Just over a dozen events and presentations delivered in the first half of 2025.

Across the entire program period to date (November 2023 – June 2025) there have been:

- **28,642 enrollees (99% of cumulative Milestone 4 target)**
- **16,416 eligible graduates (66% of cumulative Milestone 4 target) and 8,662 SME graduates (115% the Milestone 4 target)**
- **1,363 recertifications (23% of Milestone 4 target)**

There has been an improved year-on-year average time to graduate, as well as increases in program engagement.

Cyber-Wardens reporting estimates there are approximately 8,050 unique engaged small business, with at least one eligible course graduate as of 26 June 2025.* The COSBOA Member Report 2025 found a 59% conversion rate from 3,982 COSBOA contacts, resulting in 2,366 graduated.

In addition to the Milestone 4 target progress, all deliverables for Milestone 1-3 have been acquitted. Key activities include:

- Research and consultation, including research outputs and consultation reports for Disability and First Nations audience
- Course Level 2 launched, and Course Level 3 on track to launch within Milestone 4
- Cyber Wardens Champions Guide key precedent tasks completed
- Awareness and Engagement initiatives, including national webinar program, lunch and learn program, podcast season
- Student recruitment activities
- Cyber security review of the CW Google Workplace
- User experience improvements for Course Level 1
- COSBOA Roundtable

*This figure was provided by 89 Degrees East. It is based on automated cleaning and deduplication of 8,710 self-reported business names, which resulted in 8,147 unique entries after standardising case, punctuation, articles, conjunctions, and common business structure labels.

Findings – Program Outcomes

Graduates have basic technical knowledge to address and prevent common threats

Survey respondents of Course Level 1 reported high levels of likelihood to undertake actions in relation to common threats and basic technical cyber security after completing their Cyber-Wardens course. On a scale of 1-5,

- 86% (62/72) were likely or highly likely to ensure automatic updates were turned off , upgrade passwords, and apply multi-factor authentication (rating 4/5 or 5/5)
- 76% (53/72) were likely or highly likely to appoint a team member as a Cyber Warden

Graduates of Course Level 1 also reported increased understanding about Cyber security, with

- 79% (57/72) agreeing or strongly agreeing they knew more about how to safeguard their business
- 80% (58/72) had a greater understanding about small business cyber security, as well as risks for small businesses

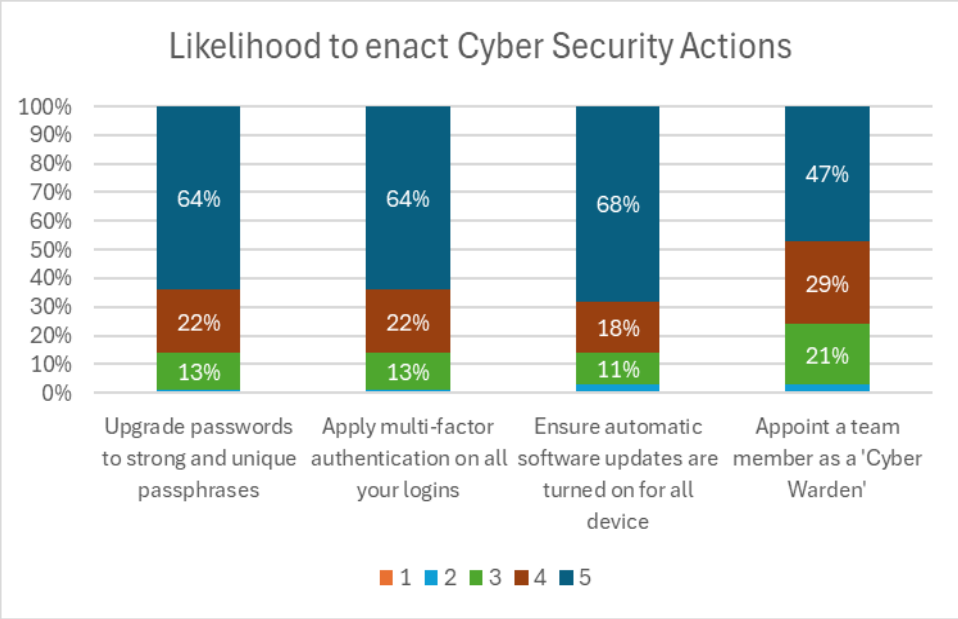


Figure 1: Graduation Survey, Course Level 1 responses to the question 'After Cyber Wardens Level 1 training, how likely are you to do the following?' with a rating of 1-5 (n=72).

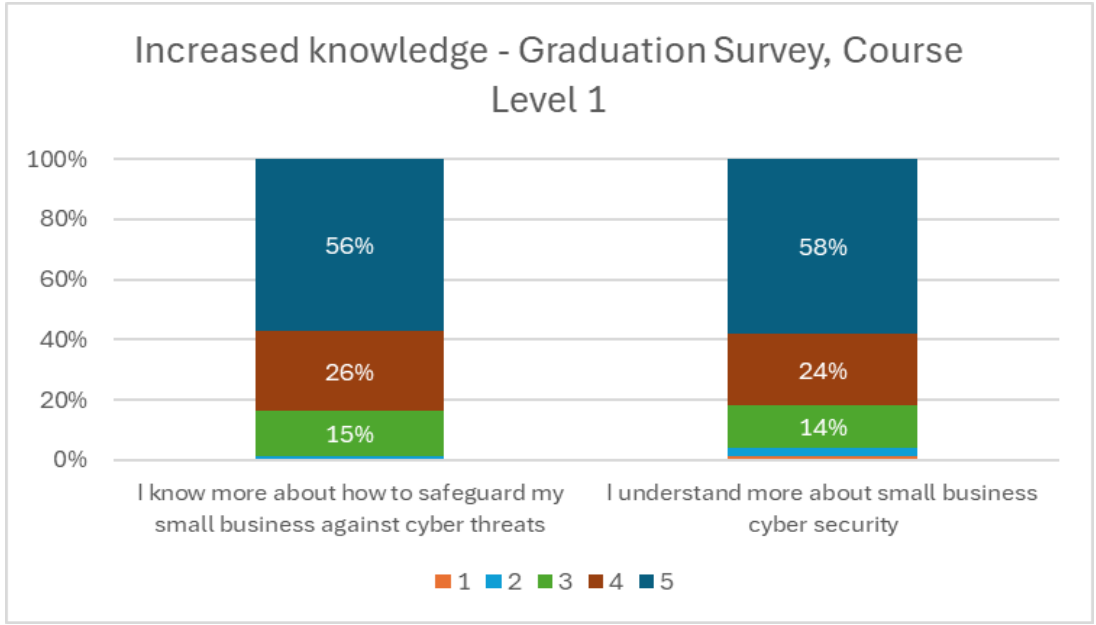


Figure 2: Graduation Survey, Course Level 1 responses to the question 'Please rate your level of agreement with the following statements between 1-5. After Cyber Wardens Level 1 Training…' (n=72).

Increased confidence to take on in-house cyber safety officer roles

There was limited direct evidence about participant confidence to take on in-house cyber safety officer roles, however as demonstrated under Mid-term outcome 4 below, there is significant evidence of increased confidence, expertise and skills to address key cyber security risks from program participants. Specifically:

- 35% (30/88) of Foundation and Course Level 1 survey respondents reported they were inspired by the training to appoint a Cyber Warden in their workplace.
- 14% (12/88) had already completed this action before participating in the Cyber Wardens course.

For the 51% (41 respondents) who reported 'not applicable', some comments reflected that it was not their responsibility to appoint staff in roles, or there were other structures in place for cyber security in their workplace. For example:

> ***I have not discussed possibility to appoint another staff member as a Cyber Warden as we do have very experienced IT onsite (Foundation Course 1, survey response).***
>
> **Foundation Course 1, Survey Response**

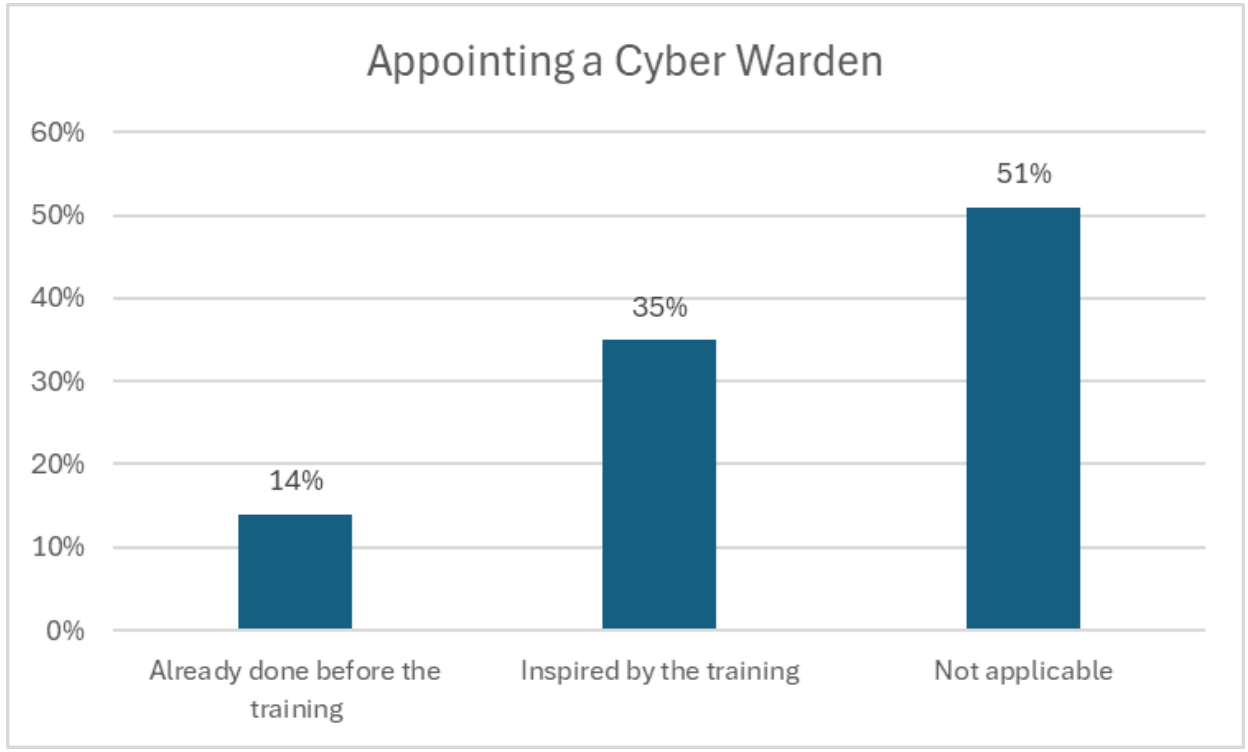


Figure 3 : Impact and Action Survey, Foundations and Course Level 1 (combined Survey 13 and 14), responses to question asking 'Have you appointed a Cyber Warden as a result of the training (n=88).

SME's see cyber security as an important internal capability

There was a significant increase in how participants viewed cyber security for their business as a result of participating in the program.

89% (159/178) of survey respondents of the Level 2 Graduation Course participants were likely or highly-likely to start conversations within their workplace about cyber-security as a result of the program.

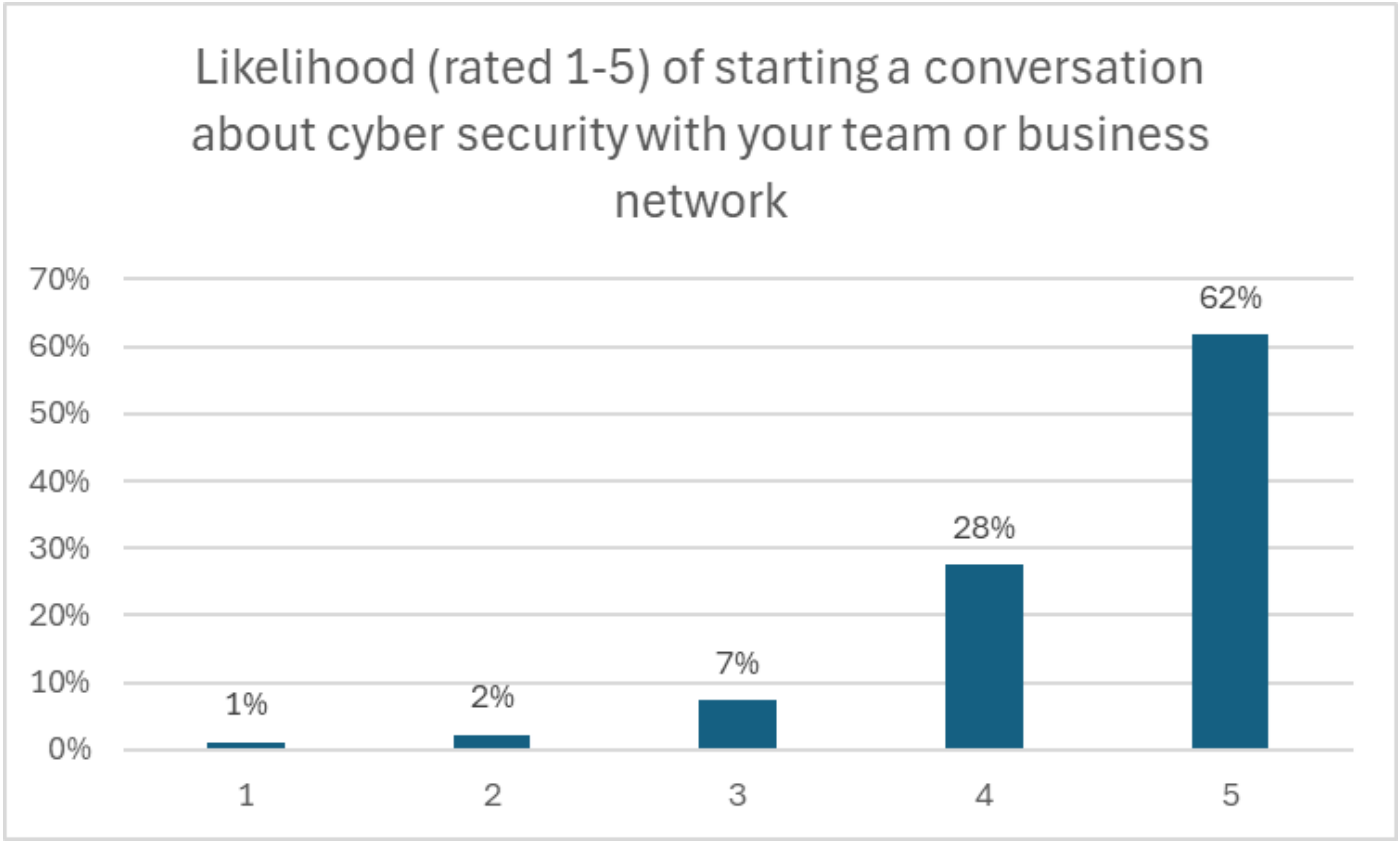


Figure 4 : Graduation Survey, Course Level 2 survey response (n=188).

SME's have demonstrable cyber security posture with employed Cyber Warden program graduates

There is a range of evidence demonstrating improvement in cyber security skills, actions and confidence as a result of participating in the Cyber Warden program.

For Course Level 2 participants, survey respondents reported that after completing their course:

- 60% (33/56) created rules or business policy for AI powered tools, 50% (28/56) were inspired to establish a secret code word, and 44% (24/56) created an incident response plan as a result of the course
- Only 25% (14/56) were inspired by the course to apply multi-factor authentication, however this was due to 73% (41/56) already doing this prior to the course.

Respondents also self-reported other actions they had taken since completing Course Level 2, including:

- **Undertaking new training with staff members (7 responses)**
- **Making AI threats a priority to discuss with staff (5 responses)**
- **Introducing a password manager (5 responses)**
- **Introduced verbal confirmation with colleagues (3 responses)**

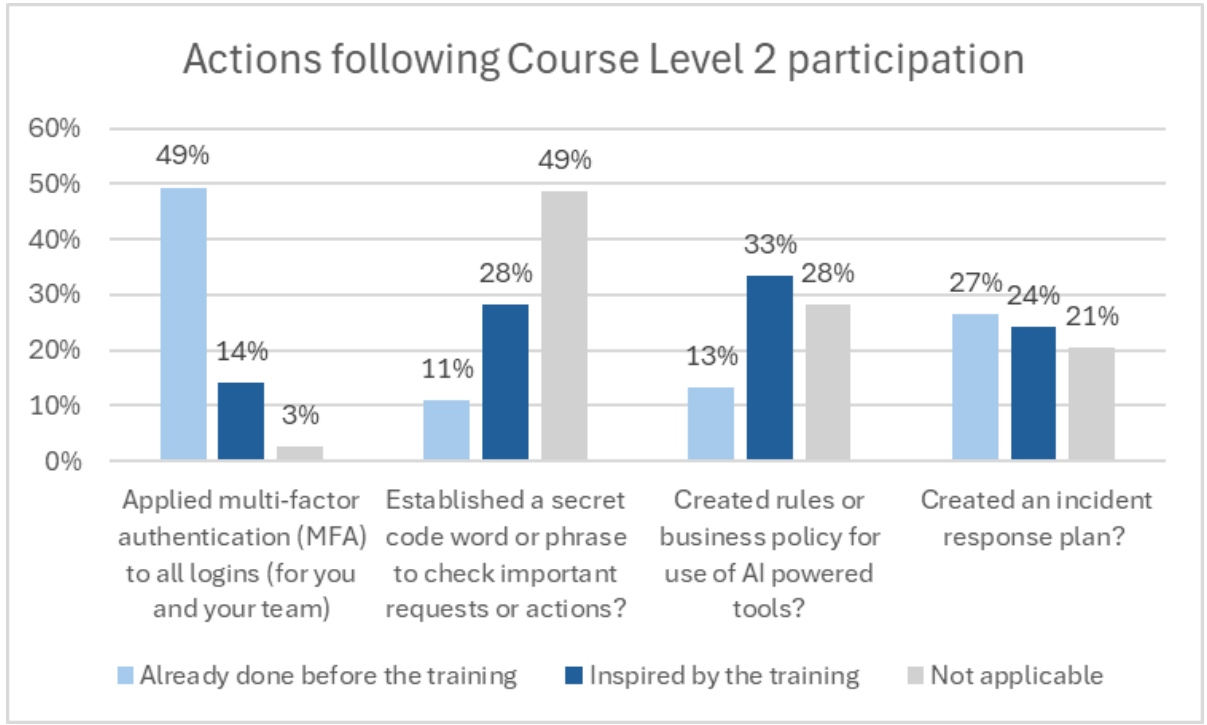


Figure 5 : Impact of Cyber Warden training on key cyber security issues, Course Level 2 (Combined 13 and 14), (n=56).

SME's have demonstrable cyber security posture with employed Cyber Warden program graduates

Course Level 2 Graduation Survey respondents had a high level of confidence to apply safe AI practices after completing the course.

- 96% (167/175) of respondents reported in increase their confidence to understand and apply safe AI practices.
- This is a significant increase to the knowledge based before completing the course, where only 19% (34/175) felt highly familiar with AI-related risks and scams.

This sentiment was also reflected in feedback from participants, where learning about AI powered phishing and scams was reported as the most valuable part of the course for protecting their business. 38 responses reflected on the threat of AI.

The section on AI-powered phishing and impersonation scams was especially useful because it explained how attackers use AI to create highly convincing fake messages and profiles. Understanding these tactics helped me recognize suspicious emails and social media contacts more quickly. Learning about malicious AI tools made me aware of the evolving threats and the importance of staying vigilant as technology advances.

Survey response, Course Level 2 Graduation Survey

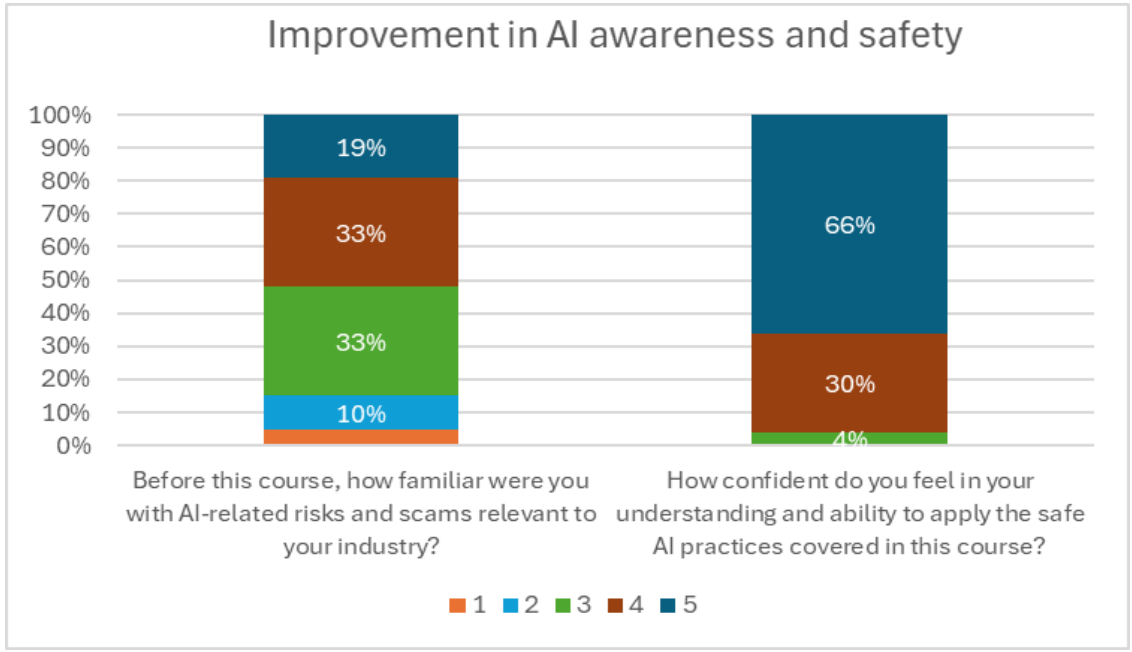


Figure 6 : Course Level 2 respondents reflecting on knowledge and confident relating to AI (on a scale of 1-5). Graduation survey (n=175).

Other valuable elements were identified in the written feedback as:

- **Scams (31 responses)**
- **Verbal passwords (14)**
- **Password attacks (12)**

SME's are empowered to engage with the Resource Hub as a source to revisit and update knowledge and skills

Across four Impact and Action survey cohorts of 144 participants, there were mixed responses about the engagement with the resource hub, with 58% of respondents accessing it a small number of times, and 35% not at all.

- Sixty-four had accessed it once or twice, and 19 had accessed it a few times (58%)
- Eight had accessed it multiple times, and 4 were still using or accessing it regularly (8%)
- Forty-nine had not accessed it at all (34%).

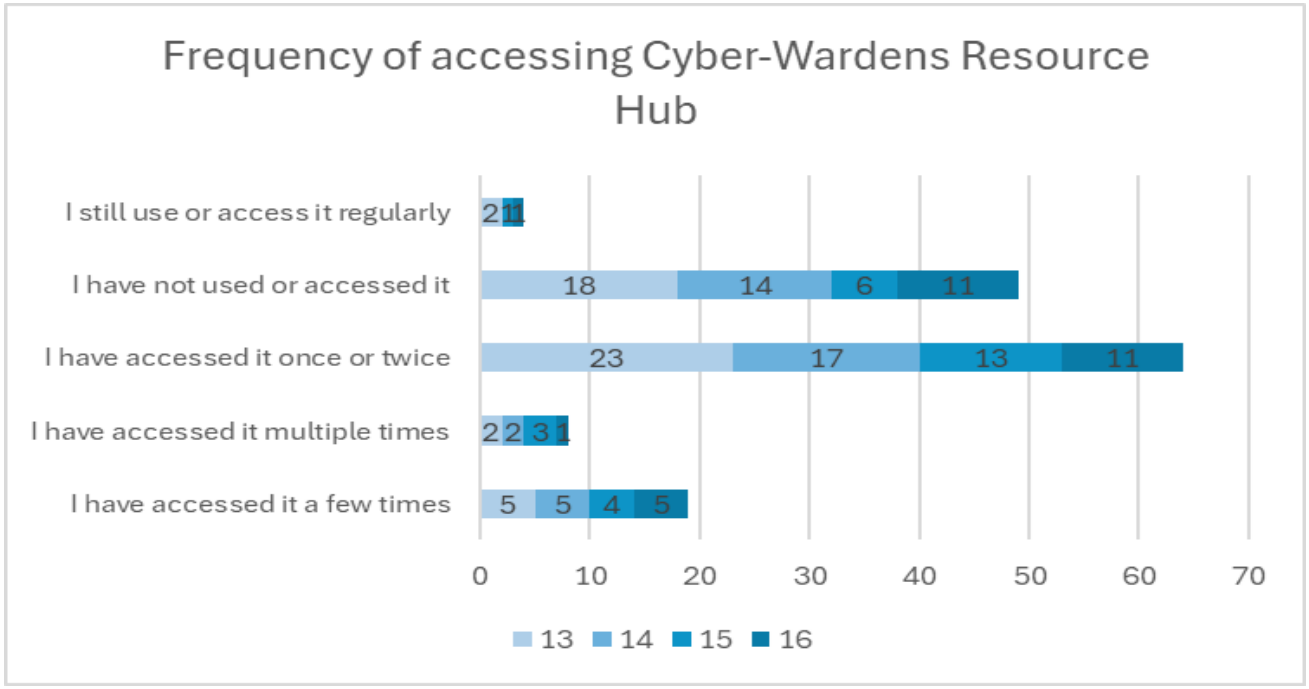


Figure 7 : Survey responses from Impact and Action Surveys (13, 14, 15 and 16 combined), (n=144).

The Resource Hub is embedded into SME operations and processes as a key source of knowledge

For those who did engage with the Resource Hub, the small business cyber tips were reported as the most valuable when selecting all valuable elements.

- 54% (78/145) respondents identified small business cyber tips as valuable (survey participants could choose multiple response options).
- 35% (51/145) valued articles on cyber threats and scams
- 33% (48/145) valued case studies, and 22% (33/145) valued guides and research

Participants also reflected on other potential resources that could be incorporated into the Hub, including

- **Aligning the resources with a suitable standard for SME's e.g., the Cyber Cert program (2 respondents)**
- **Teaching aids to use with staff (1 respondent)**
- **Platform specific content, e.g., how to safely use Google Drive (1)**
- **Provide pictograms of cyber attacks and what actions to take in response (1)**
- **Deaf/AUSLAN captioning, and use of Braille and JAW (1)**

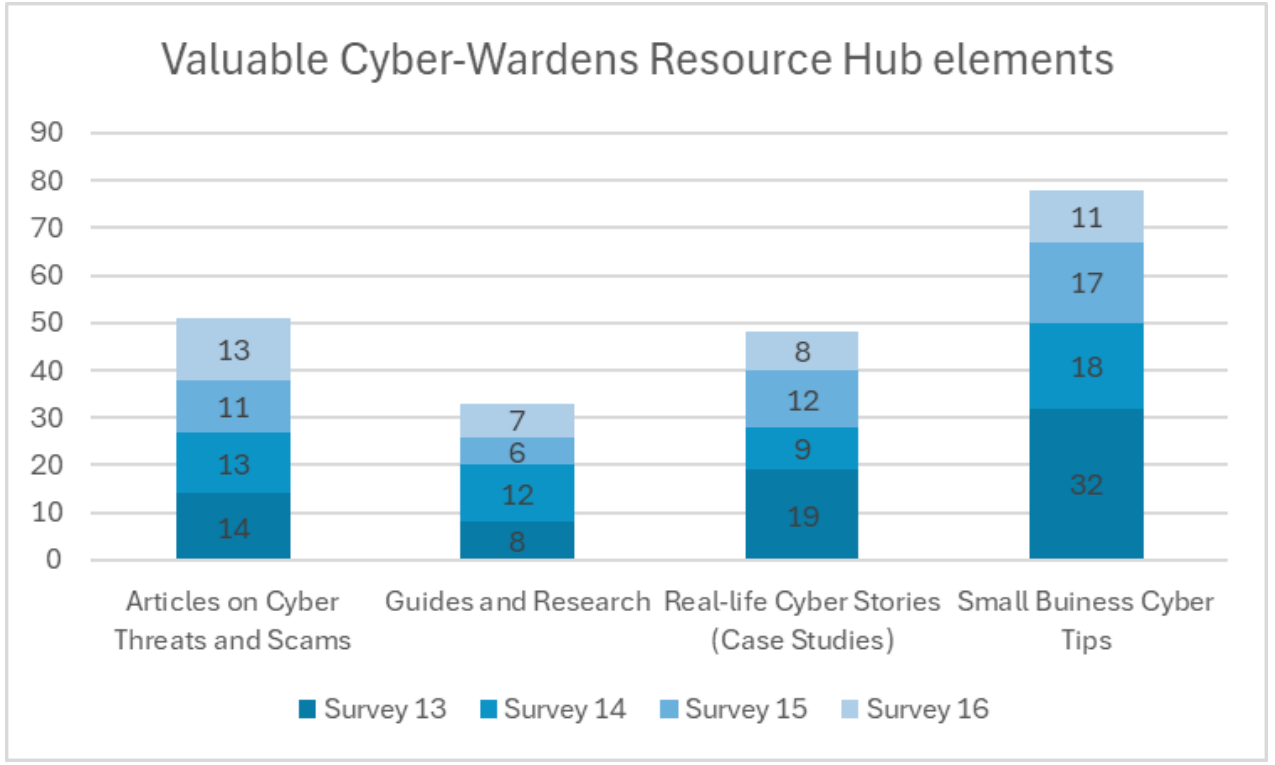


Figure 8: Multiple choice survey responses for Impact and Action Surveys (13, 14, 15, and 16) on the valuable elements of the Cyber-Wardens resource hub (n=175)

Final comments on medium-te

There is a medium-term outcome related to increases in enrolments due to increased awareness among small and medium enterprises.

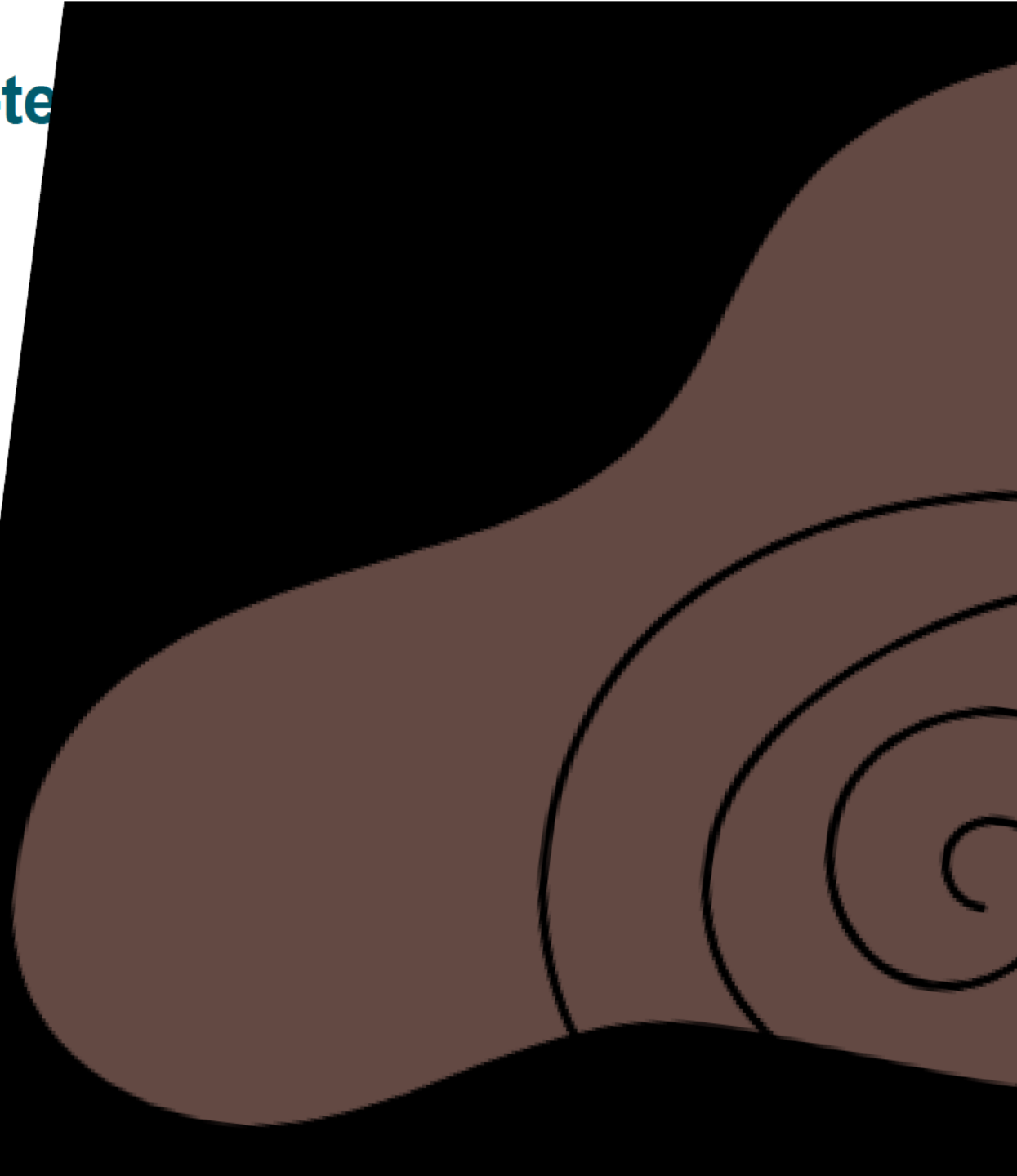
While there has been documented year-on-year growth in the uptake of Cyber Wardens, the Advisory Board has identified a risk that COSBOA member partnerships are not driving as many graduates as required to meet the cumulative eligible graduates target for Milestone 4.

There is also an identified risk of a shortfall in the number of course graduates undertaking the recertification course.

We have not commented on this further as it has been identified and various measures are noted in the report.

In terms of unintended outcomes, there were none reported by Graduate Survey respondents. However, we do note that **there were 1,363 participants from outside of the target cohort – termed 'value-add' participants.**

These included job-seekers and students (824), government organisation staff (256), charity/non-profit staff (246) and volunteers (37). Thus, these participants will still benefit broader community and organizational safety aspirations under Shield 1 of the National Cyber Security Strategy.*



* See page 16: https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy

Learnings and outcomes

Future opportunities

There is opportunity to increase awareness and engagement with the Cyber Wardens alerts. The majority of participants who responded to the Impact and Action survey were:

- Not aware of the program 34% (36/105) or,
- Had not checked them 23% (25/105).

There was very limited feedback from participants above improvements to the course. However, Graduation survey comments included:

- **A desire for more complex or 'less entry level' content (5 responses)**
- **Suggestion for self-paced options or downloadable content (3 responses)**
- **More interactive examples (2 responses)**

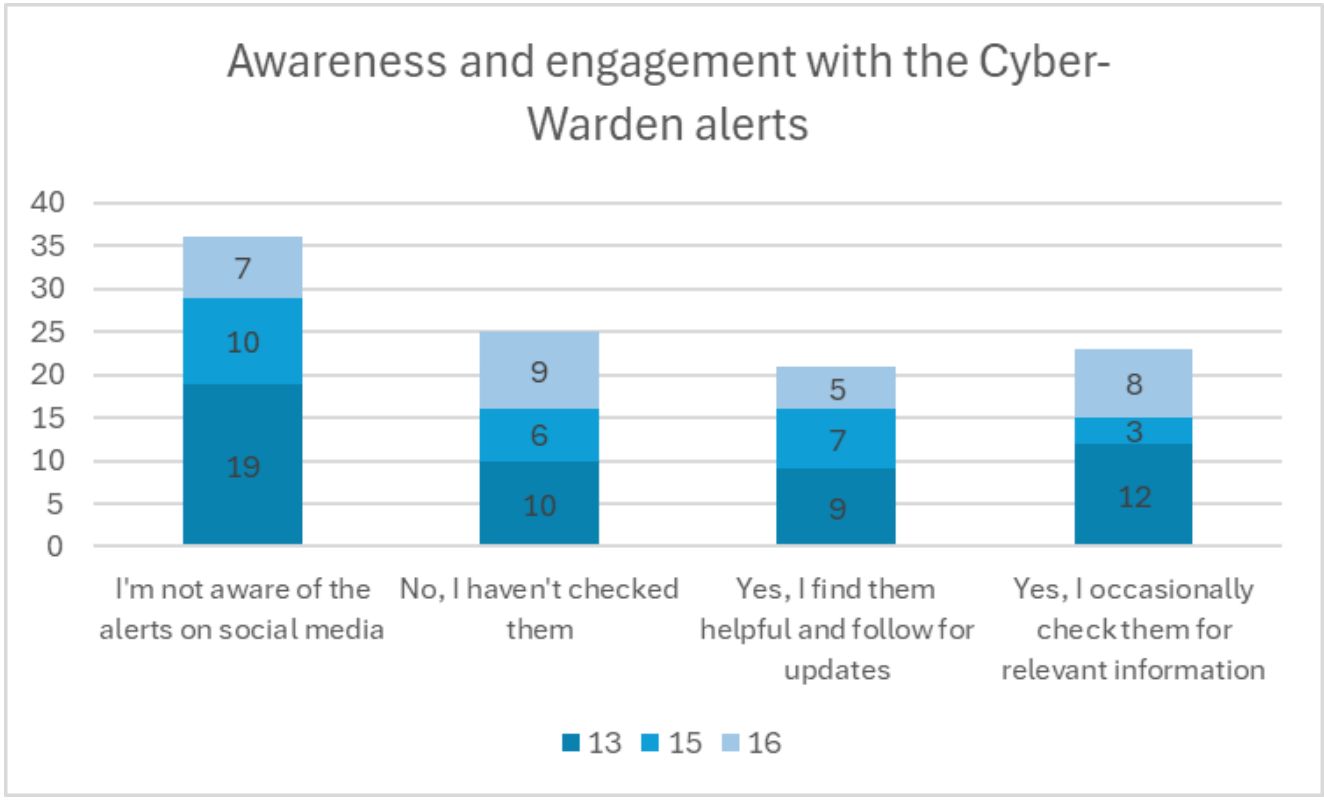


Figure 8: Impact and Action survey responses to question asking about awareness and engagement with Cyber Wardens alerts (Compiled survey ID 13,15 and 16 – survey 14 was not asked this question). n=105

Approach to the economic evaluation

How economic evaluation will be used

Economic evaluation is an approach used to determine if the benefits of a program justify the costs. There are many methods that can be used to answer different economic evaluation questions.* The evaluation of the Cyber Wardens program will utilise three types of assessment to determine the value produced. These are summarised in the table below. Our goal is to demonstrate the **realised benefits and value** – rather than assumed. The main requirements include:

- All program costs (converted to $ as much as possible) – this may mean using proxy values
- Evidence-based estimates of the costs saved / prevented (i.e. by obtaining data on the number of possible incidents that could have occurred, and an estimate of their financial and non-financial costs)
- Evidence-based estimates of the value of all other benefits produced (e.g. staff training outcomes).

Based on the data provided for this report, there will be sufficient data to develop a model to produce results as per the below three approaches. This model will be created in time for additional primary data collection – including some contingency time so that any gaps that may be identified in the program logic model outcomes can be addressed as much as possible in time for the July 2026 report.

Table 1 summarises the three methods that will be used. Table 2 over the page expands on this with more detail and examples.

Table 1: Proposed economic evaluation methods

Method	What it tells us
Cost-Effectiveness Analysis	How efficiently the program produces outputs / outcomes
Cost Avoidance Analysis	How much future cost or harm is avoided through a successful program
Cost Benefit Analysis	Whether the total financial benefits outweigh the total costs

* See the following more detail: https://evaluation.treasury.gov.au/sites/evaluation.treasury.gov.au/files/2025-07/guide-economic-evaluation-methods.pdf

How economic evaluation will be used

Table 2: Economic evaluation methods to be used

Method	Units used	What it tells us	Requires	Example	Use case
Cost-Effectiveness Analysis	$ # or % (usually)	How efficiently the program produces outputs / outcomes	• Program costs (converted to $) • Evidence of outputs (e.g. # of graduates) or outcomes (e.g. % of graduates reporting increased knowledge or skills)	s 47G(1)(a)	This allows for comparisons to other initiatives on a cost-per-output / outcome basis. This provides a common point of comparison.
Cost Avoidance Analysis	$	How much future cost or harm is avoided through a successful program	• Program costs (converted to $) • Evidence of the number of incidents (harms) prevented and their value		This is a much more focused view on the savings from prevention. In many ways it is a subset of the Cost Benefit Analysis.
Cost Benefit Analysis	$	Whether the total financial benefits outweigh the total costs	• Program costs (converted to $) • All benefits resulting from the program (relevant program logic outcomes), quantified and valued (where possible).		We can produce the net benefit (i.e. total $ value of benefit) and the cost-benefit ratio ($1 spent : $x benefit)

Conclusion and recommendations

Conclusion and recommendations

Conclusion

Overall, the data suggests that the Cyber Wardens program has built on the positive outcomes demonstrated in the first evaluation report and made progress towards intermediate outcomes. Moreover, documentation suggests a highly responsive and adaptive approach to delivery – evidenced comprehensive risk management approaches.

In particular we note outcomes related to:

- Increased technical knowledge of graduates to address and prevent common threats
- Increased understanding about small business cyber security
- A significant increase in how participants viewed cyber security for their business
- Evidence of increased cyber security skills and confidence, resulting in key actions being undertaken in SMEs
- Participants particularly valued the small business cyber tips in the Resource Hub
- The courses were viewed as the right length, using the right language, and including valuable topics.

Recommendations

In order to meet the intended program outcomes, as detailed in the logic model, by the end of the Cyber Wardens program, and based on what we observe in the data and documentation provided, there are opportunities to:

1. Continue to grow the year-on-year growth in program engagement and uptake and consider different models of recruitment to address the identified risk that COSBOA member partners are not driving as many graduates as required to meet the cumulative eligible graduates target for Milestone 4.
2. Review how to increase awareness of the Cyber Wardens alerts and Resource Hub to encourage ongoing engagement and learning.
3. Enhance program inclusivity by considering how deaf/blind participants can engage with the course, as well as options for self-paced programs or downloadable program content.

We also recognise that new program content – including the advanced course – are in development. As such, continuing to invest in ways to re-engage graduates to recertify or progress further will be important to realising the full suite of intended outcomes.

Next steps for the evaluation

Final Evaluation Report Questions

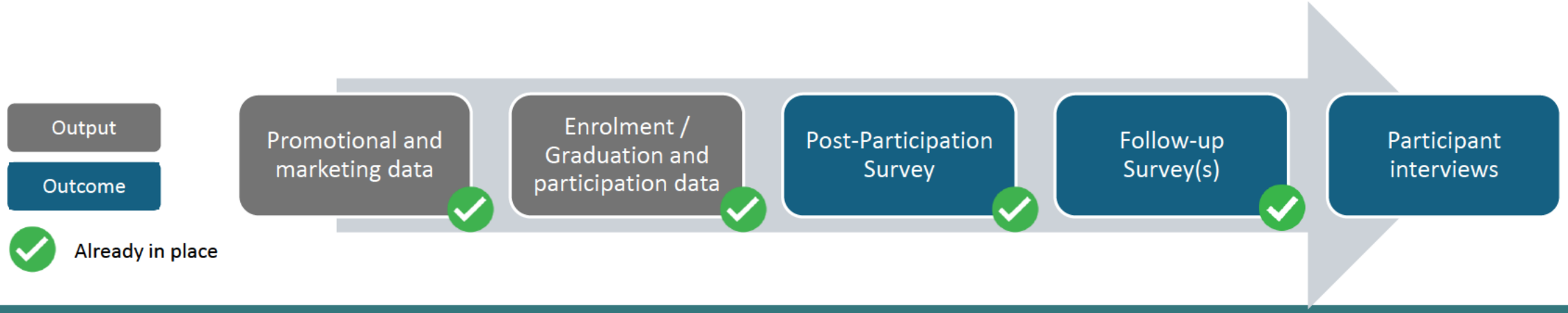
Evaluation questions provide the direction for data collection, analysis, and reporting. Our initial evaluation and this midpoint evaluation have found sufficient data has been collected that – presuming continued implementation – there will be a robust sample for the final evaluation.

The next page presents the KEQs for the final evaluation, including guiding indicators. As per the below diagram, all core data collection mechanisms are now in place (or can be replicated for new course offerings). The exception are **participant interviews**.

The goal of the interviews will be to identify exemplar experiences with the Cyber Wardens program, as well as act as a back-stop for any data gaps where survey responses were not sufficient. These will occur in the March to May 2026 period.

Final Evaluation

- **Due July 2026**
- **Final analysis of all collected data**
- **Reporting on outcomes and benefits, including economic outcomes.**



Final Evaluation

Key Evaluation Questions

Key Evaluation Questions	Sub-questions	Things to look for (indicators / measures)
Delivery **1. How well was the Cyber Wardens program delivered?**	a) To what extent were the different components of the program beneficial to participants? b) What was the total reach of the program? c) To what extent did the program meet its targets?	• Marketing and reach data • Participant engagement data (enrolments, graduations) • Participant feedback • Cost Effectiveness Analysis ($ per output)
Outcomes **2. To what extent did the Cyber Wardens program achieve its outcomes?**	a) To what extent were the intended outcomes achieved over the course of the program? b) Were there any other outcomes (positive or negative) produced? c) To what extent did the program produce value for money for the investment?	• Retention rates / engagement rates throughout the program • Proportion of attendees demonstrating improved outcomes • Net Promoter Score • Qualitative feedback indicating a good user journey / benefits from the program • Evidence of any other outcomes • Cost-Benefit Analysis and Cost-Avoidance Analysis
Future **3. What considerations are there for the future of Cyber Wardens?**	a) What has been learned that can benefit future programs in this space? b) What should happen to make the most of the benefits and outcomes from the Cyber Wardens program?	• Interpretation of collected data • Feedback from users