Eligibility criteria

Who is eligible?

To be eligible the applicant must:

- have an Australian Business Number (ABN)
- be non tax-exempt
- be registered for the Goods and Services Tax (GST)
- be operating as a viable business for a minimum 12 months

and be one of the following entities:

- a company, incorporated in Australia
- an incorporated trustee on behalf of a trust

Joint applications are acceptable, provided there is a lead applicant who is the main driver of the project, and the lead applicant is eligible to apply.

Additional eligibility requirements

Applicants must have access to, or ownership of, the intellectual property (IP) necessary to conduct the Project should it be required.

Project participants must demonstrate the financial capacity to complete the project. This must be demonstrated through the provision of financial evidence during the full application stage of the process. The portion of funding provided by AustCyber Projects Fund will be up to 50 per cent of eligible project costs.

Eligible project activities

Eligible expenditure

Projects Fund may be used for activities directly related to the project, for example:

- equipment development, testing and installation
- software development, testing and deployment
- materials, consumables and laboratory disposables
- salaries and consulting fees directly related to the activities in the project
- travel and accommodation for field activities in Australia
- capital expenditure where the equipment/works are directly related to the project.

Entities that are partly government funded such as Universities and TAFEs may apply to the Projects Fund provided that they can adequately evidence that their portion of match funding has come from commercial revenue and not from other government funding sources (e.g block grant funding).

Questions and consultation around eligible expenditure items can be obtained from AustCyber by emailing projectsfund@austcyber.com.

Ineligible expenditure

Projects Fund cannot be used for the following activities:

- indirect capital works of buildings or facilities, including
  - renovations, extensions and fit-out of buildings, unless otherwise agreed in writing with AustCyber.
- reimbursement of in-kind contributions, or to pay indirect costs of the Project such as administration costs and rent.
- international travel and salaries for international personnel, students or any overseas activities, unless the parties can demonstrate to AustCyber's satisfaction that the activities are directly related to the Project and cannot otherwise be performed in Australia.

Projects funding cannot be used to duplicate funding obtained from federal, state or territory governments but may still be included in the overall project value. Any additional government cash contributions must be matched with equal additional industry cash co-contributions.

Merit criteria

To be accepted for funding, applicants will need to address all merit criteria in their EOI application. AustCyber will assess applications against the merit criterion using a scoring framework.

Projects Fund EOIs that progress to the full Project Application stage will be asked additional questions that relate to the merit criteria listed below. The amount of detail and supporting evidence the applicant provides should be relative to the project size, complexity and project amount requested. The applicant should provide evidence to support their answers. The application forms include word limits for answers and pitches at Stage 2 will be time capped.

As a merit-based program, funding will only be awarded when Project Applications score satisfactorily against all merit criteria at each stage of the process.

Merit criterion 1

Technology Readiness Level (TRL)

The AustCyber Projects Fund can be used for early stage development of new technologies and products. Projects should start at Technology Readiness Level (TRL) of 4 or higher. Projects at a lower TRL will not be considered. Projects can also provide a solution that addresses a specific industry problem. Projects that are addressing an identified industry problem must demonstrate a TRL of no less than 5 and finish at 8 or higher.

TRL definitions can be found on the Additional Information page.

Merit criterion 2

Alignment with the Knowledge Priorities of Australia's Cyber Security Sector Competitiveness Plan

AustCyber led research identified several Knowledge Priorities in line with the current and foreseeable needs and opportunities for industry research and commercialisation in the Australian cyber security sector. These are:

1. Emerging prevention, detection and response technologies
2. Identity, authentication and authorisation in the cyber domain
3. Ensuring security, privacy, trust and ethical use of emerging technologies and services such as:
   - Cloud computing relevant
   - Cyber-physical systems, including the Internet of Things, robotics, self-driving cars etc.
   - Machine learning
   - Big data and data analytics
   - Mobile applications
4. Approaches to deal with the increasingly 'shared' responsibility of cyber security

Detailed Information on AustCyber Knowledge Priorities can be found here.

Merit criterion 3

National benefit

AustCyber has identified a need to develop certain infrastructure to sustain the growth of the cyber security sector. Applicants must be able to demonstrate how the project proposal will benefit Australia and or the broader Australian cyber security sector after project completion. The Project should have the potential to generate significant spill overs and develop world best commercial activity. Responses should demonstrate:

- The level of potential impact and contribution to the growth of the ecosystem
- Creating a champion for the sector and showcasing Australian capability both domestically and internationally
- Creating a pathway for growth for other cyber security companies
- Level of innovation/emerging technology.

Matched funding contributions

To be eligible, non-government funding from participants must fund at least 50% of the eligible project costs, either individually or collectively (if the application is made by a consortium).

Example 1:

Item	In-Kind	Cash
The industry project participants' collective contribution		$100,000
AustCyber matches financial contribution from industry		$100,000
Total project value		$200,000

Example 2:

In-kind contributions can be made by participants, but will not be included in determining the cash contribution of participants, for example:

Item	In-Kind	Cash
The industry project participants' collective contribution		$100,000
AustCyber matches financial contribution from industry		$100,000
University provides use of equipment and facilities	$50,000	
Total project value		$250,000

Example 3:

Contributions received from other government agencies, whether they are federal and/or state, do not count towards the matched funding contribution required by the project participants, and must also be matched with at least equal cash contributions. For example, if AustCyber provides Projects Fund of $100,000 and other government contributions to that project are $50,000, the minimum cash contribution required from industry participants is $150,000, for example:

Item	In-Kind	Cash
The industry project participants' collective contribution		$150,000
Government Partner (Federal and/or State or Territory)		$50,000
AustCyber matches financial contribution from industry		$100,000
University provides use of equipment and facilities	$50,000	
Total project value		$350,000

Conflicts of interest

Conflicts of interest could affect the awarding or performance of the project. A conflict of interest can be:

- real (or actual)
- apparent (or perceived)
- potential

AustCyber will ask the applicant to declare, as part of the full project application, any perceived or existing conflicts of interests or that, to the best of the applicant's knowledge, there is no conflict of interest. If the applicant later identifies that there is an actual, apparent, or potential conflict of interest, or that one might arise in relation to their project, the applicant must inform AustCyber in writing immediately.

AustCyber's conflict of interest responsibilities

AustCyber recognises that conflicts of interest may arise with our staff, technical experts, board members and others delivering the program between:

- their program duties, roles and responsibilities, and
- their private interests

AustCyber officials must declare any conflicts of interest when EOIs and Project Applications are received. Independent technical experts involved in the panel hearing project pitches (stage 2 of the process) are also subject to this.

If AustCyber identifies and considers a conflict of interest is a cause for concern, the relevant AustCyber individual or AustCyber appointed independent technical expert will not access or take part in the assessment of relevant applications under the program. AustCyber officials are compliant with conflict of interest policy as part of the Industry Growth Centres Programme Guidelines.

Intellectual property

AustCyber seeks to promote practical approaches to Intellectual Property (IP) which drives innovation, increases speed to market, and improves outcomes for the Australian cyber security sector. All Project IP will be jointly owned by the participants (excluding AustCyber) in shares proportionate to their respective contributions to the total contributions made to the project by the participants.

Project award

Project funding agreement

Successful Projects will be subject to an AustCyber Projects Funding Agreement, which is a legal contract between AustCyber and the lead project participant. The Projects Funding Agreement sets out expectations and deliverables for the project, including Project contributions and funds, reporting obligations, confidentiality, IP, Audits, GST, dispute resolution and termination.

Payments, milestones and governance

AustCyber project payments are payable by instalment, as determined by AustCyber, and may be linked to milestones defined in the Project Contract. Funding payments will be made on the basis of completion of milestones and provision of progress reports. Projects will be administered and governed according to the risk profile of the project, and as determined by AustCyber.

Reporting

AustCyber Project Governance requires participants to provide project updates for tracking actual project delivery outcomes against the cost, schedule and scope of objectives stated in the Project Agreement, on a milestone by milestone basis. AustCyber provided reporting templates must be used unless otherwise agreed by AustCyber. AustCyber reserves the right to terminate Projects funding to the project if agreed milestones are not met.

Publication

AustCyber will promote the successfully awarded projects through traditional media via media releases, social media channels, the AustCyber website, other Growth Centres, mainstream media, and an existing database of network contacts and partner networks.

AustCyber reporting obligations

AustCyber will report on the outputs and outcomes of successfully awarded projects in the AustCyber Annual Report. Once an AustCyber Project Agreement is in place, AustCyber reserves the right to publicly report on the progress and outcomes of the project, consulting with the project participants prior to doing so.

AustCyber may produce and publish a case study covering an overview of the challenges addressed, the approach, solution/learnings, and the planned benefits and general findings observed in the Project.

On project completion, the Projects Fund awardees will produce a final report, which reviews project processes, learnings, workforce training, IP, and firm level outcomes. The final report is a mandatory requirement for 'in confidence' disclosure to the Commonwealth Department of Industry, Innovation and Science and must be completed to the satisfaction of AustCyber.

AustCyber may request performance metrics on market share, entry into new markets, sales, or other data for three years post project completion.

Within 14 days of award, AustCyber is required to publish details of the Project on its website including:

- a description of the Project, and an overview of how the Project meets the strategic priorities of the Growth Centre and the objectives of the Growth Centre Projects Fund
- a list of the Project participants
- the total amount of government funding for the Project
- the total industry co-contributions for the Project.

If you have any questions, please email projectsfund@austcyber.com.