

**AI SINGAPORE**

# **ROBUST AI GRAND CHALLENGE**

Challenge Rules and Guidelines

## CONTENTS

Section 1: Introduction .....	2
Section 2: About the Challenge .....	3
Challenge Statement .....	3
Desired Outcomes and Deliverables .....	5
Additional Support .....	5
Section 3: Programme Details .....	6
Programme Structure .....	6
Funding Support .....	7
Application Process .....	8
Evaluation Process .....	10
Additional Remarks .....	10
Section 4: How to Participate .....	11
Eligibility .....	11
Submission .....	12
Section 5: Other Information .....	13
Intellectual Property .....	13
Ethics and Confidentiality .....	14
Project Support and Facilitation .....	14
Frequently Asked Questions (FAQ) .....	14
Contact Information .....	15

## SECTION 1: INTRODUCTION

- 1.1 AI Singapore's Robust AI Grand Challenge ("the Challenge"), organised in collaboration with the Future Systems and Technology Directorate (FSTD), MINDEF Singapore, and DSO National Laboratories, is a competitive research funding initiative that supports the development and adoption of innovative approaches and Artificial Intelligence (AI) techniques that address the vulnerabilities of AI models in Computer Vision (CV) systems for Autonomous Vehicles (AV).
- 1.2 The objective is to increase the robustness of AI models against real-world adversarial attacks, in 3 key CV tasks commonly used in AVs : (i) object detection, (ii) stereo-depth estimation, and (iii) semantic segmentation.
- 1.3 The Challenge is open for the six (6) Singapore-based Institutes of Higher Learning (IHLs)<sup>1</sup> and A\*STAR Research Institutes. Proposals are invited from multidisciplinary teams and consortia of academics, researchers, scientists, engineers, domain experts, and other professionals. Teams are also encouraged to involve collaborators from public agencies and/or the industry.

---

<sup>1</sup> Institutes of Higher Learning (IHLs): National University of Singapore (NUS), Nanyang Technological University (NTU), Singapore Management University (SMU), Singapore University of Technology and Design (SUTD), Singapore Institute of Technology (SIT), Singapore University of Social Sciences (SUSS)

## SECTION 2: ABOUT THE CHALLENGE

### CHALLENGE STATEMENT

2.1 The challenge statement is as follows:

***“How can we design robust CV systems for AVs that can recover at least 80% of their original accuracy<sup>2</sup> after physical testing-time adversarial attacks?”***

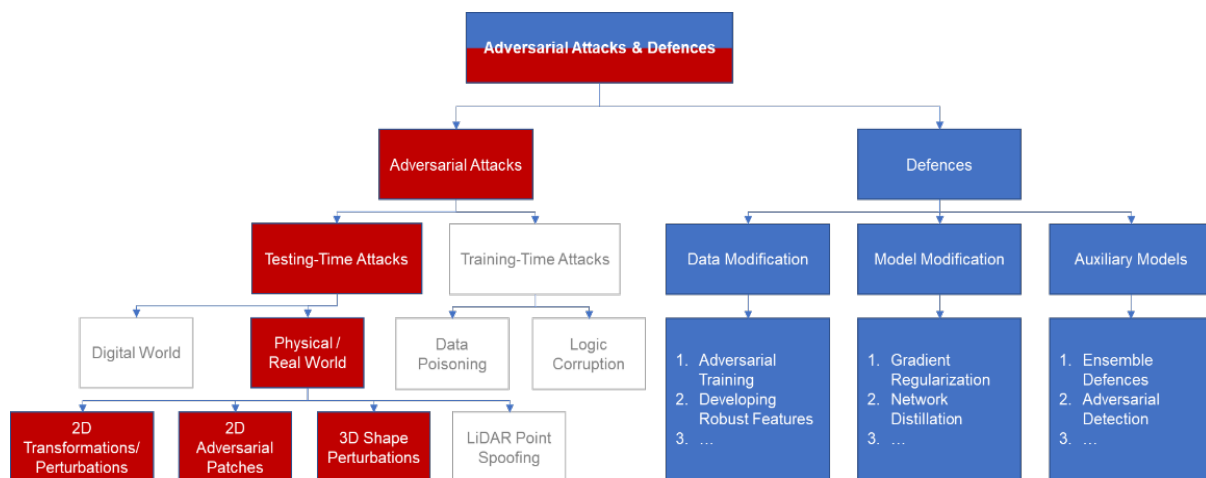
- 2.2 CV systems based on machine learning are increasingly integral in a wide range of applications, including security and surveillance and AVs. However, these systems are vulnerable to adversarial attacks which could compromise safety and security, thus limiting their performance and adoption in critical environments. In the field of AVs, these attacks could lead to delays, accidents, and even death.
- 2.3 While CV systems in AVs are multi-sensor, existing research on adversarial attacks, and hence defences, has mostly focused on addressing single-sensor attacks and attacks in the digital space, which are typically not applicable in real-world scenarios.
- 2.4 The goal is to increase the robustness of AI models against adversarial attacks that are applicable in the physical space, thereby increasing the safety and security, and hence adoption of AI in CV systems in critical environments.
- 2.5 In this Challenge, the focus is on three (3) key CV tasks that are commonly deployed in AVs, namely:
- i) **Object Detection:** Detection of specific objects of interest<sup>3</sup>.
  - ii) **Stereo Depth Estimation:** Estimation of distance between the AV to objects of interest, using a stereo camera setup.
  - iii) **Semantic Segmentation:** Recognising a collection of inputs to form specific distinct categories of interest.

<sup>2</sup> Original accuracy refers to the accuracy of a non-robustified model before attacks (i.e. clean accuracy).

<sup>3</sup> Examples of objects of interests are, but not limited to, pedestrians, vehicles, obstacles, buildings, traffic signs.

2.6 Teams should describe the following in their full proposals<sup>4</sup>:

- i) **Baseline CV Models:** These refer to the vanilla AI models that are used to address the key tasks identified in Para 2.5, free of any adversarial training or robustification.
- ii) **Adversarial Attacks:** The Challenge will focus on a subset of adversarial attacks and defences illustrated in red and blue in the image below. However, teams are encouraged to propose other novel techniques that are not highlighted below, as long as they tackle the key focus areas.



Each team will minimally need to address 3 classes of physical, testing-time attacks, which are:

- 2D transformations/perturbations
- 2D adversarial patches
- 3D shape perturbations

- iii) **Defences:** The Challenge will focus on the following 3 types of defences:
  - Data modifications
  - Model modifications
  - Auxiliary models

Teams can also propose additional defences that can be practically implemented in the physical world.

2.7 For the purposes of this Challenge, it can be assumed that the adversary has no access to, nor knowledge of, the target system's models, including its training processes and parameters, data, and digital input.

<sup>4</sup> More details will be shared at the grant briefing workshop.

- 2.8 The Challenge requires close collaboration between AI scientists from various computer vision sub-domains, and DSO domain experts to develop dual-use technologies with civilian and military applications.

#### DESIRED OUTCOMES AND DELIVERABLES

- 2.9 The desired outcome is to advance the state-of-the-art for robustification of AI models applied in multi-sensor CV systems, in real-world scenarios. The deliverable for each team is a suite of multi-modal (camera and LiDAR) attack and defence techniques that can be implemented and deployed in the real world.
- 2.10 Teams will be given opportunities to participate in physical trials as part of the progress review<sup>5</sup>. Additionally, as part of the final performance review, teams will deploy their techniques in the real world, and all teams will red-team one another's defences. Black-box attacks on all teams' defences will also be conducted.<sup>6</sup>
- 2.11 The team should conform to general guidelines for reproducible research and include a code and data management plan. The newly created and non-proprietary parts of the solution should be ready to be packaged for general distribution, for further development or commercialisation.
- 2.12 The techniques developed must not infringe on the intellectual property rights of others; reasonable steps must be taken to ensure that all the components or subsystems can be used, and if appropriate, included for distribution according to the Terms and Conditions of the AI Singapore Grand Challenge Funding Scheme.
- 2.13 The resulting Intellectual Property (IP) will be governed by the terms and conditions of the AI Singapore Grand Challenge Funding Scheme (refer to Section 5: Other Information).

#### ADDITIONAL SUPPORT

- 2.14 During Stage 1, AISG, in collaboration with DSO, will release annotated camera and LiDAR data, collected from real-world environments in Singapore. This will help teams to train and test their models virtually, prior to the physical trials.

During Stage 1, teams will be given opportunities to trial their developed techniques in the real world. Additional details on the trial sites and frequency will be released to awarded teams in Stage 1 once finalised.

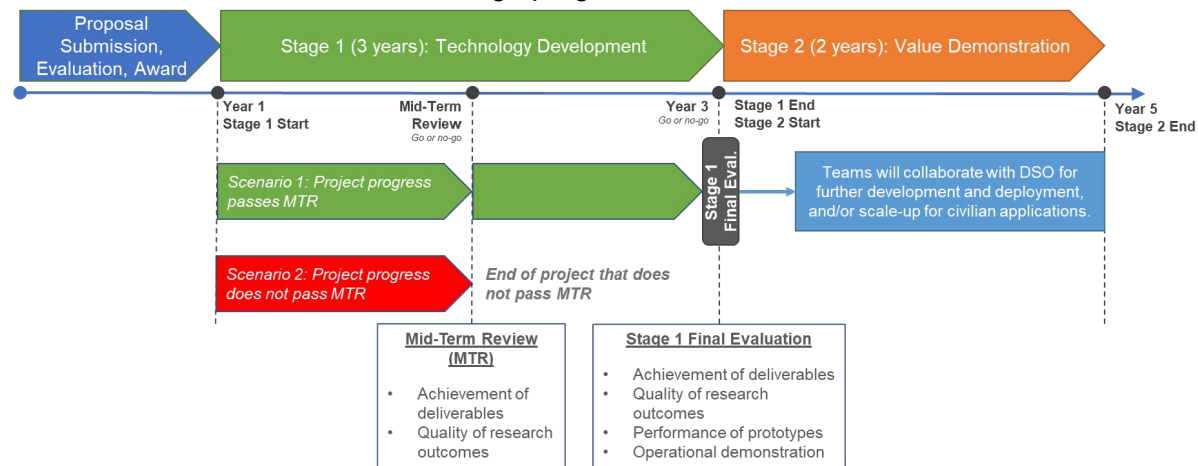
<sup>5</sup> More details will be shared at the grant briefing workshop.

<sup>6</sup> The suite, approach and complexity of adversarial attacks will not be made known to the teams, but solutions should minimally be robust against attacks that are already highlighted in Para 2.6 (ii).

## SECTION 3: PROGRAMME DETAILS

### PROGRAMME STRUCTURE

3.1 The Robust AI Grand Challenge programme structure is illustrated below:



The challenge will adopt a 2-stage developmental approach:

#### Stage 1: Technology Development

3 teams will be funded up to S\$4M each, over 3 years.

Access to real-world data and physical trials will be provided.

#### Stage 2: Value Demonstration

Selected team(s) could be funded up to S\$5M over 2 years.

Teams will have the opportunity to work with agencies to adapt and scale up the developed AI techniques for dual-use applications.

3.2 For Stage 1 (Technology Development), awarded teams will be funded to develop AI techniques to address the challenge statement. AISG and DSO will work closely with the awarded teams to implement the developed techniques in a real-world environment and provide feedback to the teams' research and development.

3.3 Three (3) selected teams will each receive grant support of up to S\$3 million for the first two (2) years of Stage 1, i.e. Stage 1a.<sup>7</sup> Each team will undergo a mid-term review on its project progress (approx. 18 months into the challenge), to assess if the team is eligible for the remaining S\$1 million grant support over the last one (1) year of Stage 1, i.e. Stage 1b.

<sup>7</sup> Request for no-cost grant extension for Stage 1a is strictly not allowed. Any unutilised funds from Stage 1a will not be rolled over to Stage 1b. Final reports (incl. final expense claims, final KPI report and final progress report) for Stage 1a shall be provided to AI Singapore latest by 31 Jul 2025 (i.e. one month after the end of Stage 1a).

- 3.4 Nearing the end of Stage 1 (approx. 30 months into the challenge), these teams will undergo a final performance review, which will be taken into consideration when assessing a team's eligibility for further grant support in Stage 2.
- 3.5 In Stage 2 (Value Demonstration), teams could (i) work closely with DSO for further development and deployment, and/or (ii) scale up the developed techniques for civilian applications. A separate funding will be used to support the work in Stage 2.

#### FUNDING SUPPORT

- 3.6 Funding support will only be for Stage 1: Technology Development only. The total duration proposed shall not exceed three (3) years, and the corresponding budget requested (inclusive of Indirect Research Costs (IRC)), shall not exceed S\$4 million.
- 3.7 Only activities conducted in Singapore may be funded under the AI Singapore Grand Challenge Funding Scheme.
- 3.8 The proposal shall be based on a realistic budget with appropriate justifications that correspond to the scope of work to be accomplished. The total cost of each project includes all approved direct costs<sup>8</sup> and indirect research costs/overheads<sup>9</sup>. All expenditure budgeted should be inclusive of any applicable Goods and Services Taxes (GST) at the prevailing rates.
- 3.9 For all direct cost items proposed, please note that:
- Host Institutions must strictly comply with their own procurement practices.
  - Host Institutions must ensure that all cost items are reasonable and are incurred under formally established, consistently applied policies and prevailing practices of the host institution.
  - All items/services/manpower purchased/engaged must be necessary for the R&D work.
- 3.10 Lead PI/Co-PIs/Host institutions shall use reasonable efforts to employ or otherwise engage Singapore citizens and/or Singapore Permanent Residents to be deployed in the work under the project.

<sup>8</sup> Direct costs are defined as the incremental cost required to execute the project. This excludes in-kind contributions, existing equipment and the cost of existing manpower as well as building cost. Supportable direct costs can be classified into expenditure on manpower (EOM), expenditure on equipment (EQP), other operating expenses (OOE), overseas travel (OT) and research scholarship (RS).

<sup>9</sup> Indirect costs are expenses incurred by the research activity in the form of space, support personnel, administrative and facilities expenses, depending on the host institution's prevailing policy. Host institutions will be responsible for administering and managing the support provided by AI Singapore for the indirect costs of research. This will not be applicable to research scholarship.



- 3.11 Please refer to Annex A – Guidelines for the Management of Research Grants (AISG) for more information, include the list of “Non-fundable Direct Costs”.

#### APPLICATION PROCESS

- 3.12 The timeline for the Robust AI Grand Challenge is shown in the table below:

Role	Timeline
Grand Challenge launch	1 Dec 2022
AISG Grant Management System (GMS) open for submissions	By 1 Mar 2023
Deadline for submission	31 Mar 2023, 1800hrs (SGT)
Proposal evaluation by Evaluation Committee	Apr – Jun 2023
Release of outcome and award	Jun 2023
Grand Challenge Stage 1 Start	1 Jul 2023

- 3.13 Parallel submissions are not allowed, i.e., applicants must not send similar versions or part(s) of the current proposal application to other agencies or grants for funding (or vice versa).
- 3.14 Research support office from the IHLs and/or Research institutes are required to ensure that information submitted by their researchers is complete and compliant with the requirements outlined in the application guidelines. Failure to do so will result in rejection without review.
- 3.15 Only complete applications with the endorsement of the relevant institutional authority or director of research (or equivalent), received before the closing date for submission, will be accepted by AI Singapore.

3.16 The completed application should comprise the following documents.

Document	Comments
<b>Full Proposal</b>	<ul style="list-style-type: none"> <li>• Must be endorsed by relevant institutional authority or director of research (or equivalent).</li> <li>• Must not exceed 10 pages and adhere to the prescribed format and address the points as stated in the templates provided.</li> <li>• Elaboration of a proposal's content within appendices will not be considered.</li> </ul>
<b>Recorded Presentation</b>	<p>A recorded presentation is also required for submission (in .mp4 format only)<sup>10</sup>, and shall adhere to the following guidelines:</p> <ul style="list-style-type: none"> <li>• Its duration is strictly limited to 10 minutes. Any content beyond the 10-minute mark will not be considered.</li> <li>• Teams are to focus on the following aspects of the proposal: <ul style="list-style-type: none"> <li>○ Scientific novelty</li> <li>○ AI techniques proposed</li> <li>○ Team's data strategy</li> <li>○ Team's expertise, and how the team is leveraging existing capabilities and resources to deliver success.</li> </ul> </li> </ul>
<b>Budget</b>	<ul style="list-style-type: none"> <li>• Completed according to the template provided</li> </ul>

<sup>10</sup> The recorded presentation(s) shall be uploaded to a platform and a download link shall be provided to AI Singapore by the submission deadline. File size shall be minimised.

## EVALUATION PROCESS

- 3.17 Full Proposals will be reviewed by the AISG Grand Challenge Evaluation Committee (EC), based on the quality of the proposals in the following key aspects:
- Scope of proposed project
  - Significance and potential impact of project
  - Data availability and access
  - Test plans and test suites
  - Team expertise
  - Outcomes and deliverables
  - Risk assessment and mitigation
  - Potential deployment pathway
- 3.18 All applicants will be notified of the outcome. However, due to the volume of applications, we will not be able to provide feedback to unsuccessful applicants. All decisions are final, and no appeals will be entertained.
- 3.19 AI Singapore reserves the rights to terminate, at any point in time, a project that does not meet the minimum expectations of progress and achievement, upon recommendation by the Evaluation Committee. The Evaluation Committee may also make recommendations to maximise the outcomes of funded projects.

## ADDITIONAL REMARKS

- 3.20 Teams are strongly encouraged to have experts with the right skills and experience, and to involve collaborators from relevant public agencies and/or industries to strengthen the potential of deployment pathways.
- 3.21 Teams are strongly encouraged to source for and utilise additional data sources to deliver the project. These could include, but are not limited to, open-sources of data, data obtained by the teams through various collaborations, or additional data collection activities planned by the team.
- 3.22 At the grant call briefing on 3 Jan 2023, AI Singapore will provide more details on the datasets to be released, trials and reviews to be conducted. Prospective applicants are strongly recommended to attend or send a suitable representative. The recordings, materials, and any Q&A answered during the briefing will also be shared via our AI Singapore website after the event.

## SECTION 4: HOW TO PARTICIPATE

### ELIGIBILITY

- 4.1 Each eligible host institution<sup>11</sup> may submit:
- No more than three (3) applications each for NUS, NTU and A\*STAR.
  - No more than one (1) application each for SMU, SUTD, SUSS and SIT.
- 4.2 Each team must consist of one (1) Lead Principal Investigator (Lead PI) and at least one (1) Co-Principal Investigator (Co-PI). The eligibility for each role within the research team is described below:

Role	Eligibility
<b>Lead PI</b>	<ul style="list-style-type: none"> <li>• Must hold a full-time appointment<sup>12</sup> and be salaried in a Singapore-based IHL or an A*STAR Research Institute.</li> <li>• Lead PI must have extensive background and qualifications in the field of Artificial Intelligence.</li> </ul>
<b>Co-PI</b>	<ul style="list-style-type: none"> <li>• Co-PIs must hold a full-time appointment and be salaried in a Singapore-based IHL or Research Institutions<sup>13</sup>.</li> <li>• At least one of the Co-PIs must be a subject matter expert in the domain.</li> </ul>
<b>Collaborator</b>	<ul style="list-style-type: none"> <li>• Any member that brings value to the team, but does not fall under the Lead-/Co-PI eligibility (refer to Para 4.3 and 4.4 for additional requirements), such as but not limited to: <ul style="list-style-type: none"> <li>○ Collaborators from public or private sector.</li> <li>○ Overseas collaborators or visiting experts.</li> </ul> </li> </ul>

- 4.3 Overseas collaborators and/or visiting experts should spend sufficient time in Singapore to build up a strong local research group in new areas with the assistance of a local principal investigator to ensure continuity.
- If the visiting expert plays a major role in the AI Grand Challenge project, he/she should be based in Singapore for at least six (6) months each year.
  - Alternatively, the overseas collaborators and/or visiting experts may be invited to Singapore on short-term engagements to assist with specific project tasks. In either arrangement, the costs of airfare, accommodation and per diem can be budgeted under the other operating expenses of the AI Grand Challenge project.

<sup>11</sup> The host institution is determined based on where the Lead PI is holding a full-time appointment in.

<sup>12</sup> Defined as at least 9 months of service a year based in Singapore or 75% appointment.

<sup>13</sup> Research Institutes include A\*STAR Research Institutes and CREATE entities.

- Staff of overseas collaborators can be hired directly through the local IHLs as full-time visiting research fellows (or equivalent). The staff must be based in Singapore for at least one (1) year.
- 4.4 Partnering industry organisations must have presence in Singapore to be considered as collaborators. At least 1 signatory from each listed collaborating organisation must also be based in Singapore to facilitate communications and accountability. Collaborating companies with no presence in Singapore may only be considered if supported with very strong justifications.
- 4.5 Notwithstanding the above, AI Singapore strongly encourages international collaborations and may consider alternative special arrangements proposed by the Lead PI.

#### SUBMISSION

- 4.6 Only one member from each research team can submit the application. This is to facilitate the planning and organisation of the information and the proposal review process. The applicant will be the primary contact for the team.
- 4.7 The application must be submitted by the Host Institution to AI Singapore via the AI Singapore's GMS Portal, which will be open to receive submissions from 1 Mar 2023 onwards.
- 4.8 The closing date for submission is 31 Mar 2023, 1800hrs (SGT).

## SECTION 5: OTHER INFORMATION

### INTELLECTUAL PROPERTY

- 5.1 Intellectual Property (“IP”) developed under the Challenge (“Research IP”) shall be co-owned by the Institutions and Collaborators in accordance with their inventive or creative contributions, where such agreed terms shall be set out in a written agreement between the Institutions. The Investigators and Collaborators shall identify and disclose to the Institutions, details of all such Research IP.
- 5.2 The Institutions shall keep and maintain a fully comprehensive and updated list of all such Research IP and make such details available to AI Singapore and/or the grantors for inspection at any time.
- 5.3 The Institutions shall grant AISG Limited, a company limited by guarantee and responsible for the management, exploitation and commercialisation of Research IP, a non-exclusive, non-transferable, sub-licensable, perpetual, irrevocable, worldwide, royalty-free right and license to use, modify, reproduce and distribute the Research IP (excluding any Research IP that is solely developed by a Collaborator) for research, development and/or commercial purposes (the “AISG License”).
- 5.4 Except the rights expressly licensed or otherwise provided in this Challenge Rules & Guidelines or the terms and conditions of the AI Singapore Grand Challenge Funding Scheme, the Institutions shall in any event retain all rights, title and interest in all Research IP and shall have the free and unfettered right to use and commercialise (which include granting licenses to third parties) the Research IP for any purpose on a non-exclusive basis without seeking the consent of AI Singapore and AISG Ltd.
- 5.5 Management of all Research IP shall have reference to and be guided by the AI Singapore IP Policy. In general, Research IP may be open-sourced for research and experimentation and licensed for commercial deployment.
- 5.6 The Institutions shall use best efforts to ensure that the Research IP is properly managed and wherever feasible, fully exploited and commercialised (including being made available for research and development or commercial purposes). Where required to do so by AI Singapore, the Institutions shall attend such meetings as AI Singapore may direct to discuss the potential for exploitation and commercialisation of Research IP.
- 5.7 The Institutions shall reserve a royalty-free, irrevocable, worldwide, perpetual and non-exclusive right for the Singapore Government and public sector agencies and DSO National Laboratories to use any licensed Research IP for their statutory functions, non-commercial and R&D purposes.

## ETHICS AND CONFIDENTIALITY

- 5.8 All the Investigators, Collaborators, staff, and students working on the project must comply with the relevant local laws or regulations governing the research.
- 5.9 All teams are responsible for ensuring that ethical issues relating to their respective projects are identified and brought to the attention of the relevant regulatory bodies for approval. Approval to undertake the research must be granted before any work requiring approval begins.
- 5.10 Ethical issues should be interpreted broadly and may encompass, among other things, relevant codes of practice, the involvement of human participants, tissue or data in research, the use of animals, research that may result in damage to the environment and the use of sensitive economic, social or personal data.
- 5.11 The work should be conducted under strict international, national, and/or institutional guidelines on privacy and confidentiality protection of personal data use.
- 5.12 Whenever possible, all datasets used should be de-identified and anonymised, and/or proper consents and approvals should be obtained for the use of the data.
- 5.13 All the Investigators, Collaborators, staff, and students working on health- and biomedical-related projects should obtain CITI certification (<https://about.citiprogram.org/en/homepage/>) on biomedical data use or similar training and certification.
- 5.14 Researchers and research institutions should recognise that they have an ethical obligation to weigh societal benefits against risks inherent in their work. All research must be conducted responsibly and honestly. Researchers should also refer to their own research institution's guidelines on ethical conduct/research integrity.
- 5.15 All participating parties must fully comply with the AI Singapore Robust AI Grand Challenge Rules & Guidelines, Terms and Conditions of the AI Singapore Grand Challenge Funding Scheme, and Terms and Conditions of the AISG License.

## PROJECT SUPPORT AND FACILITATION

- 5.16 Where possible, AI Singapore may facilitate or support project work in the following areas:
- Expert advice and consultation (from technical experts)
  - Project management

## FREQUENTLY ASKED QUESTIONS (FAQ)

5.17 Appended are the answers to FAQs that we have received

**Qns: What is the Indirect Research Cost (IRC) support rate?**

Ans: Institutions selected to host Grand Challenge projects will be eligible for IRC funding of (i) 20% for the first 2 years of Stage 1 (Stage 1a), and (ii) 30% for the last 1 year of Stage 1 (Stage 1b), of the direct cost approved under the AI Singapore Grand Challenge Funding Scheme.

Do note that:

- The S\$4 million funding cap for Stage 1 is inclusive of the IRC as described above; and
- Unutilised funds from Stage 1a will not be rolled over to Stage 1b.

**Qns: Does the grant support Research Scholarships (RS)?**

Ans: RS are eligible for grant support under this Challenge, for the period of Stage 1a (i.e. up till 30 Jun 2025) and Stage 1b (i.e. 1 Jul 2025 to 30 Jun 2026). Do note that grant support for RS in Stage 1b will also be subject to the mid-term review as mentioned in Para 3.3.

**Qns: Does the grant support Lead PI's and Co-PI(s)' salaries?**

Ans: Lead PI's and Co-PI(s)' salaries are not eligible for grant support under this Challenge.

**Qns: Are collaborators and partners eligible to receive funding from the grant?**

Ans: Collaborators and partners are not eligible to receive funds from the AI Singapore Grand Challenge Funding Scheme.

**CONTACT INFORMATION**

5.18 For any enquiries, please contact [grandchallenge@aisingapore.org](mailto:grandchallenge@aisingapore.org), attn: Robust AI GC.