CyberSG R&D Programme Office (CRPO)

GRANT CALL RULES AND GUIDELINES

1. Overview

1.1. The CyberSG R&D Programme Office (CRPO) is a new national centre at Nanyang Technological University, Singapore. CRPO will focus its efforts on three main thrusts to advance cybersecurity comprehensively: cutting-edge research and development, advancements in technology and translational development, and fostering ecosystem/industry growth and training.

1.2. CRPO aspires to propel Singapore to the forefront of cybersecurity innovation and implementation, fuelled by funding from the Cybersecurity Agency of Singapore (CSA). This financial backing empowers CRPO to finance visionary projects proposed by diverse entities, including Research Institutes based in Singapore (RIs), Institute of Higher Learning (IHLs), and Industries based in Singapore. The scope of these initiatives spans the entire Technology Readiness Level (TRL) spectrum, from nascent concepts at TRL 1 to advanced, field-tested solutions at TRL 9, all within the dynamic realm of cybersecurity.

1.2.1. CRPO serves as a key research translation centre, driving the conversion of research into tangible outcomes. It establishes a strong governance framework for translational activities, fosters an inclusive ecosystem for talent development and communication, and collaborates with NTUitive Pte Ltd ("NTUitive") to streamline IP management. CRPO aims to create a user-friendly policy framework for SMEs and MNCs, facilitating the adoption of innovative cybersecurity inventions. It is more than a funding entity, acting as a catalyst for the holistic advancement of Singapore's cybersecurity landscape.

1.2.2. In Frontier Research and Development, the emphasis is on enhancing core cybersecurity capabilities through fundamental research and addressing societal challenges with moon-shot initiatives. Translation and Industry-Driven Technology Development involve translating fundamental research into commercial potential, creating a local cybersecurity innovation platform, and catalyzing industry growth through grant management and collaborations with governmental and private partners.

1.2.3. The third thrust, Translation and Innovation, aims to demonstrate cybersecurity capabilities. Translation and Innovation will be done through incubators, training, and hackathons, while providing cybersecurity technology training to industries and schools. CRPO aims to raise awareness and adoption of cybersecurity technologies, develop a strong talent pool, and facilitate talent flow across sectors through various schemes.

1.3. CRPO is set to initiate the CRPO Grant Call – Grand Challenge to back the advancement of cyber technologies and innovation addressing tangible issues with transparency and accountability. The goal is to generate national benefits for Singapore.

1.4. The CRPO Grant Call is a competitive funding initiative aimed at fostering research projects that push the boundaries of cyber technologies within Singapore-based Institutes of Higher Learning (IHLs)[1], Research Institutes (RIs)[2], and Industry Partners[3]. We enthusiastically invite proposals from diverse and collaborative teams, including academics, researchers, scientists, engineers, domain experts, and other professionals, to contribute to the advancement of cutting-edge cyber technology science.

1.5. For details regarding the timeline of the CRPO Grant Call - Grand Challenge and the submission deadline for proposals, kindly review paragraph 6.7.

2. Scope of Grant Call

2.1. Aligned with the aforementioned goals and directions, this grant call will concentrate on cybersecurity research.

2.2. **Grand Challenges Grants:** This pillar aims to foster the creation of innovative approaches and groundbreaking research ideas that address challenges with substantial industrial and societal impact. These projects align with the strategic direction set by the government, holding national strategic importance in both the short and long term. Ideally, these projects correspond to current (if short-term) or future (if long-term) governmental challenges or initiatives. For instance, cybersecurity technologies may target and develop solutions for challenges in healthcare, focusing on awareness and education for children and the elderly. These initiatives supplement and leverage government programs such as the smart nation initiative.

2.3. The proposed opportunities and focus areas shall include:

2.3.1. **AI Security** The proliferation of foundation models, such as OpenAI's GPT-4 [1] and PaLM [2], has significantly transformed the landscape of Natural Language Processing and Artificial Intelligence.

[1] Institutes of Higher Learning (IHLs): Such as 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), (refer to the complete list here: https://www.ica.gov.sg/reside/LTVP/apply/graduate-from-an-institute-of-higher-learning-seeking-employment-in-singapore/list_ihl).

[2] Research Institutes (RIs): Such as the Agency for Science, Technology and Research (A*STAR) institutes.

[3] Industry Partners: Singapore based companies and Singapore based Start-ups.

By learning patterns from vast amounts of data, these models have demonstrated remarkable success in understanding and generating human-like text across diverse vertical industrial scenarios such as finance service, healthcare, electronics, and smart city management. However, the widespread deployment of foundation models has engendered a series of novel cyber-attack challenges that could have profound consequences for society, security, and privacy. Addressing these challenges is crucial to ensure the responsible and safe use of foundation models in an era characterized by digital ubiquity.

2.3.1.1. *Challenges:*

2.3.1.1.1. **Adversarial Manipulation:** Adversarial attacks exploit vulnerabilities in foundation models by introducing carefully crafted input perturbations, leading to incorrect or misleading outputs [3]. These attacks pose a significant threat, potentially enabling malicious actors to generate deceptive content, evade detection, or manipulate automated systems.

2.3.1.1.2. **Data Poisoning:** Data poisoning attacks represent another significant challenge. Malicious actors may attempt to manipulate the training data used to build foundation models, embedding biased or misleading information. As a result, the model's outputs may inadvertently perpetuate stereotypes, misinformation, or discriminatory content. Data poisoning attacks not only undermine the reliability of foundation models but also erode societal trust and exacerbate existing biases.

2.3.1.1.3. **Privacy Breaches:** Foundation models, often trained on large and diverse datasets, might inadvertently expose private or sensitive information contained within their learned representations [4]. Ensuring robust privacy-preserving mechanisms during training and deployment is essential to prevent unintended data leakage.

2.3.1.1.4. **Transfer Learning Vulnerabilities:** Pre-trained foundation models are commonly fine-tuned for specific tasks, and such transfer learning can introduce vulnerabilities. Cyber-attacks targeting transfer learning processes can potentially compromise model performance, introduce bias, or lead to unintended behaviours [5].

2.3.1.2. ***Goals:*** To overcome the mentioned challenges, the primary goal of the Grand Challenge related to this subject is to investigate innovative and efficient resolutions that guarantee the responsible and secure use of foundational models in significant applications. The proposed solution should encompass the following dimensions.

2.3.1.2.1. **Adaptive Adversarial Training:** Incorporating adversarial training techniques [6] can enhance foundation model robustness against adversarial attacks, making the model more resistant to input perturbations.

2.3.1.2.2. **Robust Data Validation:** Implementing rigorous data validation and verification mechanisms can help detect and mitigate data poisoning attempts during the training phase.

2.3.1.2.3. **Privacy-Preserving Architectures:** Exploring privacy-preserving techniques, such as differential privacy or federated learning [7], can safeguard sensitive information while maintaining foundation model utility.

2.3.1.2.4. **Fine-Tuning Security:** Developing secure and auditable fine-tuning procedures can reduce the risk of vulnerabilities introduced during the transfer learning process [8].

References

[1] OpenAI, *“GPT-4 Technical Report”, arXiv preprint arXiv:2303.08774* (2023).

[2] Chowdhery, Aakanksha, Sharan Narang, Jacob Devlin, Maarten Bosma, Gaurav Mishra, Adam Roberts, Paul Barham et al. "Palm: Scaling language modeling with pathways." *arXiv preprint arXiv:2204.02311* (2022).

[3] Formento, Brian, Chuan-sheng Foo, Anh Tuan Luu, and See Kiong Ng. "Using Punctuation as an Adversarial Attack on Deep Learning-Based NLP Systems: An Empirical Study." In the Association for Computational Linguistics: EACL 2023, pp. 1-34. 2023.

[4] Zhao, Wayne Xin, Kun Zhou, Junyi Li, Tianyi Tang, Xiaolei Wang, Yupeng Hou, Yingqian Min et al. "A survey of large language models." *arXiv preprint arXiv:2303.18223* (2023).

[5] Zhao, Shuai, Jinming Wen, Anh Tuan Luu, Junbo Zhao, and Jie Fu. "Prompt as Triggers for Backdoor Attack: Examining the Vulnerability in Language Models." arXiv preprint arXiv:2305.01219 (2023).

[6] Dong, Xinshuai, Anh Tuan Luu, Rongrong Ji, and Hong Liu. "Towards robustness against natural language word substitutions." *In Proceedings of International Conference on Learning Representations (ICLR)* (2021).

[7] Fowl, Liam, Jonas Geiping, Steven Reich, Yuxin Wen, Wojtek Czaja, Micah Goldblum, and Tom Goldstein. "Decepticons: Corrupted transformers breach privacy in federated learning for language models." *arXiv preprint arXiv:2201.12675* (2022)

[8] Dong, Xinshuai, Anh Tuan Luu, Min Lin, Shuicheng Yan, and Hanwang Zhang. "How should pre-trained language models be fine-tuned towards adversarial robustness?." *Advances in Neural Information Processing Systems (NeurIPS)* (2021).

2.3.2. **Secure and Private Data Sharing** In the dynamic landscape of technology, data sharing [1] stands as a pivotal driver of innovation in AI driven intelligent systems [2], cloud computing [3], and blockchain [4]. Fueling AI's learning algorithms and predictive power, diverse datasets enhance accuracy across sectors like healthcare and finance. Cloud computing's scalability and collaboration thrive on shared data, fostering cost-effective and accessible solutions. Meanwhile, blockchain's decentralized ledger hinges on data sharing for transparent and secure transactions, impacting supply chains and finance. These intertwined technologies collectively rely on data sharing to break the data-silo and unlock groundbreaking advancements. In shaping the future, strategic data sharing remains integral to realizing the full potential of these transformative forces for the betterment of society. However, ethical, security and privacy concerns [5] underline the need for responsible implementation. It is vital to achieve security guards against breaches and cyber threats, while privacy safeguards protect personal information and uphold regulatory compliance. Simultaneously, prioritizing fairness prevents biased outcomes and discriminatory practices, particularly crucial in intelligent systems. Collectively, these principles foster trust, minimize risks, and sustain ethical practices in data sharing, nurturing a responsible technological landscape.

2.3.2.1. *Challenges*

2.3.2.1.1. **Security of Data Sharing for Intelligent Systems**: Rare existing approaches can guarantee the data confidentiality, integrity, and availability (CIA) [6] simultaneously to provide provable secure data sharing for AI driven intelligent systems.

2.3.2.1.2. **Privacy Concerns in Cloud Computing:** Numerous deployed applications tend to abuse user data, undermine privacy, and violate regulations (e.g., GDPR) [7]. Large-scale shared data introduce significant privacy concerns. Existing schemes lacks analyzable private data sharing framework with rich functionalities.

2.3.2.1.3. **Reliable Fairness Guarantees**: Reliable contribution evaluation and incentive mechanisms [8] for large-scale data sharing frameworks like Blockchain and Intelligent Systems lacks sufficient efforts, which is the foundation of project commercialization.

2.3.2.1.4. **Efficiency Boosting**: The co-design of algorithm and hard-ware acceleration is rarely touched in existing approaches. High efficiency is paramount for all the intelligent systems or novel computing paradigms such as Cloud and Blockchain.

2.3.2.2. ***Goals:*** To address the aforementioned obstacles, the primary objective of the Grand Challenge pertaining to this subject is to explore innovative and efficient resolutions that ensure the security, privacy, and fairness of the existing data sharing framework within significant applications. The proposed solution should encompass the subsequent dimensions.

2.3.2.2.1. **Secure Data Sharing for Intelligent Systems:** It aims to (1) develop confidential computing framework for the sharing of large-scale training data, (2) design formal integrity verification mechanisms for the diverse training and inference paradigms, (3) present provable robustness enhancing methods for various data sharing functions with confidential and integrity guarantees.

2.3.2.2.2. **Private Data Sharing in Cloud Computing:** It aims to (1) investigate e Provable private preserving algorithms with rich data sharing functionalities, (2) devise fine-grained and dynamic access control mechanism that can restrict data sharing to selected individuals/groups, (3) explore private large-scale data sharing as a service enabling diverse cloud driven applications.

2.3.2.2.3. **Fairness Guarantees for Data Sharing in Blockchain and Intelligent Systems:** It aims to (1) design reliable contribution evaluation mechanisms, (2) devise deployable incentive mechanisms for large-scale Blockchain and Intelligent System, (3) integrating provable security and privacy guarantees for fair data sharing.

References

[1] Kalkman S, Mostert M, Gerlinger C, et al. Responsible data sharing in international health research: a systematic review of principles and norms [J]. BMC medical ethics, 2019, 20: 1-13.

[2] Chen J, Sun J, Wang G. From unmanned systems to autonomous intelligent systems [J]. Engineering, 2022, 12: 16-19.

[3] Sun P J. Security and privacy protection in cloud computing: Discussions and challenges [J]. Journal of Network and Computer Applications, 2020, 160: 102642.

[4] Lu Y, Huang X, Dai Y, et al. Blockchain and federated learning for privacy-preserved data sharing in industrial IoT [J]. IEEE Transactions on Industrial Informatics, 2019, 16(6): 4177-4186.

[5] Makhdoom I, Zhou I, Abolhasan M, et al. PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities [J]. Computers & Security, 2020, 88: 101653.

[6] Dylan D H. CIA and the Pursuit of Security: History, Documents and Contexts [M]. Edinburgh University Press, 2020.

[7] Lu C, Liu B, Zhang Y, et al. From WHOIS to WHOWAS: A Large-Scale Measurement Study of Domain Registration Privacy under the GDPR [C]. NDSS. 2021.

[8] Yin B, Wu Y, Hu T, et al. An efficient collaboration and incentive mechanism for Internet of Vehicles (IoV) with secured information exchange based on blockchains [J]. IEEE Internet of Things Journal, 2019, 7(3): 1582-1593.

2.4. The grant applicants is responsible for defining the proposed research, problem scope, technical approach, and potential impacts of the proposal. Additionally, proposals must explicitly address the following key points:

- Alignment of the proposal with CRPO's objectives and direction.
- Explanation of the novelty of the research and the significant research challenge it aims to address.
- Clarification of potential industry applications or impact.
- Presentation of the translation plan.
- Explanation of the relevance of the research to Singapore.

3. Funding Support

3.1. CRPO intends to unveil two grand challenges aimed at soliciting innovative approaches to enhance the cybersecurity landscape of both Singapore and the global community. The initiative seeks breakthrough research ideas that can propel advancements in cybersecurity technologies. Each challenge offers funding of up to Singapore Dollars Six Million ($6,000,000) for a selected grant applicant, supporting a duration of 2.5 to 3 years for each project.

3.2. The first call was released on 12th December 2023. Please look at section 6 for the planned timeline of Grand Challenge Grants.

3.3. The proposal shall be based on a realistic budget with appropriate justifications that correspond to the scope of work to be accomplished.

3.4. The corresponding budget requested **includes** 30% Indirect Research Costs (IRC).

3.5. The total cost of each project includes all approved direct costs[4] and indirect research costs/overheads[5]. All expenditure budgeted should be inclusive of any applicable Goods and Services Taxes (GST) at the prevailing rates.

3.6. For all direct cost items proposed for the project, please refer to Annex C – Guidelines for the Management of CRPO Grants, including the list of "Non-Fundable Direct Costs" and note the following:

- 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.

3.7. Research Scholarships are not eligible for support under the CRPO Grant Call.

3.8. Funds awarded cannot be used to support overseas R&D activities. All funding awarded must be used to carry out the research activities in Singapore.

4. Project Deliverables and Outcomes

4.1. Each project is expected to produce most, if not all, the following deliverables:

- Translation, Technologies deployed, including licences.
- Publications in top tier journals and conferences.
- Industry R&D jobs.
- PhDs and Masters trained.

[4] 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) and overseas travel (OT).

[5] 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 CRPO for the indirect costs of research, if any.

4.2 In addition to the above deliverables, grant applicants may state deliverables applicable to the project.

5. Eligibility

5.1. The grant call is open to researchers from all Singapore-based Institutes of Higher Learning (IHLs), Research Institutes (RIs) and Industry Partners[6].

5.2. At the point of application, the Principal Investigator (PI) must hold a full- time[7] appointment in one of the eligible institutions. The PI must be a subject matter expert in the proposed domain, with strong record of publications in the proposed domain's conferences and journals.

5.3. Lead PI must be from the IHLs or the RIs and the Co-PI can be from the Industry Partners.

5.4. If applicable, Co-PIs must hold a full-time appointment in one of the eligible institutions at the point of application. At least one of the Co-PIs must be a subject matter expert in the proposed domain. For industry partner, the Co-PIs must hold full-time appointments at the company.

5.5. Researchers from Medical Institutions[8], Singapore based companies and Singapore based Start-ups, private sector, and other entities are eligible to apply as Collaborators.

5.6. Company collaboration(s) with in-kind contributions is encouraged, but not compulsory.

5.7. The team must have the right skills and experience to deliver the project and demonstrate sufficient engagement with stakeholders to scope the proposal.

5.8. The overseas collaborators and/or visiting experts may be invited to Singapore on short term engagements to assist with specific project tasks. In this arrangement, the costs of airfare, accommodation and per diem can be budgeted under the other operating expenses of the project.

5.9. Only research conducted in Singapore may be funded under CRPO Grant Call - Grand Challenge. Please refer to Annex B – Terms and Conditions of CRPO Grant.

[6] 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), A*STAR Research Institutes, Singapore based companies and Singapore based Start-ups.

[7] Defined as at least 9 months of service a year based in Singapore or 75% appointment.

[8] Researchers from Medical Institutions in Singapore who hold at least 25% joint appointment in a Singapore-based IHL and/or A*STAR RI may apply as Lead PI or Co-PI. If awarded, the grant will be hosted in the IHL / A*STAR RI.

5.10. Lead PI and Co-PIs should note that parallel submissions are not allowed – i.e., applicants must never send similar versions or part(s) of the current proposal application to other agencies or grants for funding (or vice versa). The proposals should not be funded, or currently considered for funding, by other agencies. Details of all grants currently held or being applied for by the Lead PI and Co-PIs in related areas of research must be declared in Annex A - CRPO Grant Call Proposal Template.

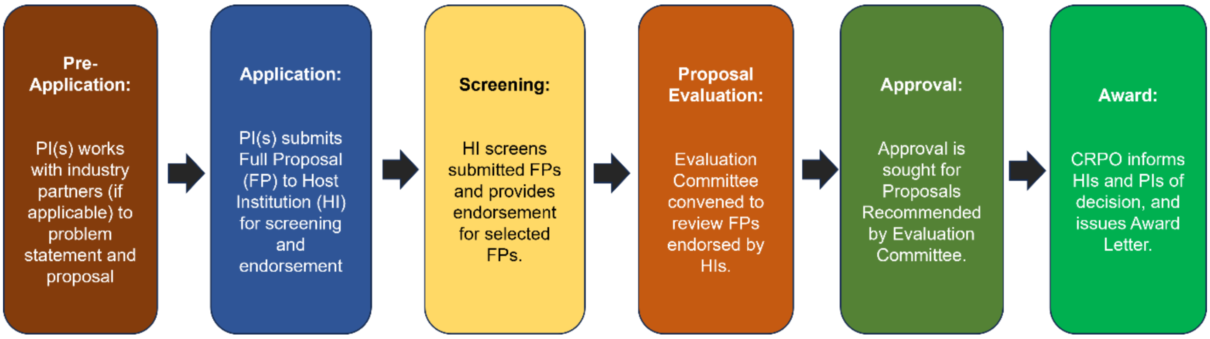
6. Review and Selection

6.1. Full proposals are to be submitted using the Proposal Template for CRPO Research Call in Annex A and must also adequately address the pointers stated therein.

6.2. Full proposals will be reviewed by the Evaluation Committee, based on the quality of the proposals in the key aspects listed in paragraph 2.4 as well as the following:

- Past research accomplishments of the PI, Co-PI and any collaborators
- Project management plan

6.3. An illustration of the application, review and selection process is shown below:



Pre-Application: PI(s) works with industry partners (if applicable) to problem statement and proposal

Application: PI(s) submits Full Proposal (FP) to Host Institution (HI) for screening and endorsement

Screening: HI screens submitted FPs and provides endorsement for selected FPs.

Proposal Evaluation: Evaluation Committee convened to review FPs endorsed by HIs.

Approval: Approval is sought for Proposals Recommended by Evaluation Committee.

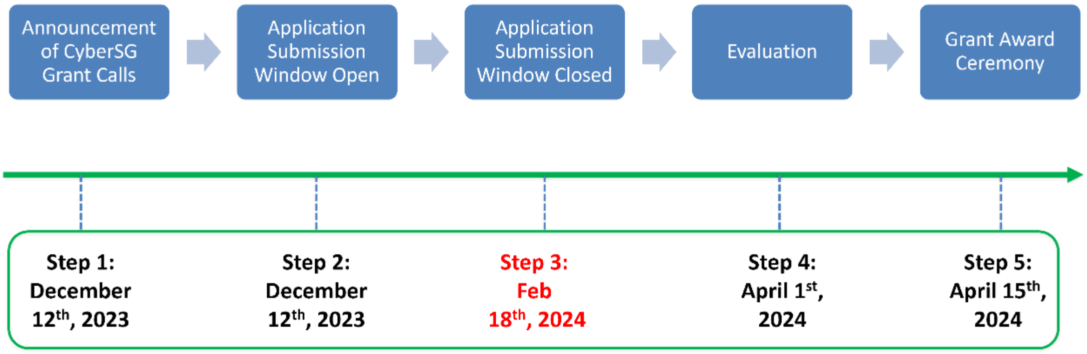
Award: CRPO informs HIs and PIs of decision, and issues Award Letter.

6.4. The review will be carried out by the CRPO Evaluation Committee but based on reviews of the proposals solicited from local and overseas experts.

6.5. Reviewers should not be asked to review proposals from their affiliated institutions.

6.6. The review process is expected to take approximately 6 weeks. All decisions are final, and no appeals will be entertained.

6.7. The timeline[9] for this CRPO Grant Call is shown below:


Announcement of CyberSG Grant Calls
Application Submission Window Open
Application Submission Window Closed
Evaluation
Grant Award Ceremony
Step 1: December 12th, 2023
Step 2: December 12th, 2023
Step 3: Feb 18th, 2024
Step 4: April 1st, 2024
Step 5: April 15th, 2024

6.8. Please note that respective IHLs' or RIs' internal deadline for full proposal submission may differ. However, all proposals selected and endorsed by the Host Institutions must be submitted in via email to CRPO@ntu.edu.sg according to the above timeline.

6.9. CRPO reserves the right to reject late or incomplete submission, and submissions that do not comply with application instructions.

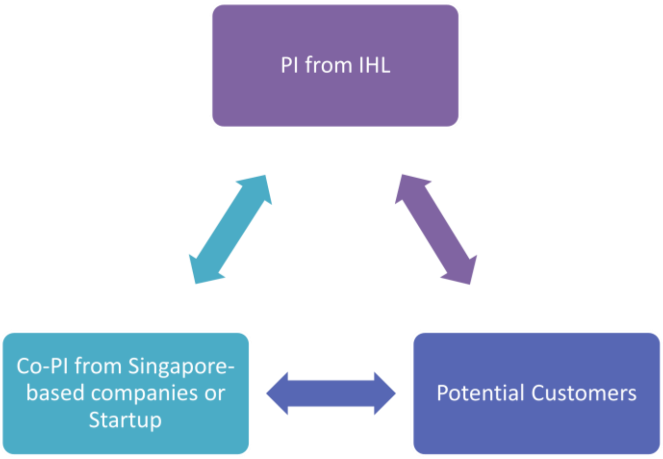
7. Team Structure

7.1. One Lead-PI from Singapore-based Institutes of Higher Learning (IHLs) and Research Institutes (RIs) to conduct fundamental research.

7.2. One industry Co-PI from Singapore-based companies or startup to identify and translate IPs with commercial potential.

7.3. Potential customer collaborators who are willing to adopt the developed security solutions and provide requirement feedback.

7.4. An illustration of the team structure and the collaboration between the teams is shown below:



[9] Timeline is subject to change and based on CRPO decisions.

8. Research Project Performance Assessment

8.1. Successful teams will undergo a mid-term review on its project progress approx. 12 months into the challenge.

8.2. Funding for Stage 2 will only be unlocked upon satisfactory progress.

8.3. Nearing the end of Stage 2, approx. 24 months into the commercialization, the team will undergo a final review.

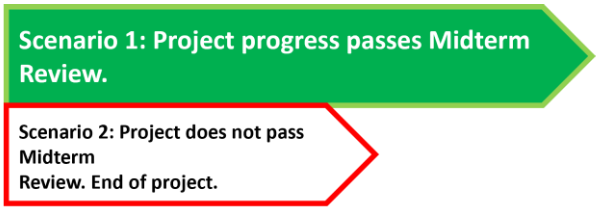
8.4. Eligibility for further support in Stage 3 will be assessed based on final review.

8.5. Nearing the end of Stage 3, approx. 36, the team is expected to provide mature products atop the R&D outputs.

8.6. Receive benefits from marketplace and enter a virtuous cycle of R&D and commercialization.

8.7. The performance and potential of the team's research project will be evaluated during a midterm review, which will be carried out by the Evaluation Committee before the end of 12 months. The interim review will be conducted approximately 24 months into the project. Teams will be required to give a presentation for the review. The project will be assessed primarily based on the progress of promised deliverables and quality of research outcomes.

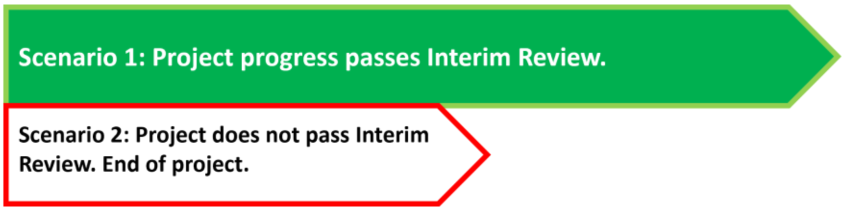
8.8. If the team passes the midterm review, funding support for the team to continue the research project will be made available. CRPO reserves the rights to terminate, after midterm review or at any point in time, a project that does not meet the minimum expectations of progress and achievement, upon recommendation by the Evaluation Committee.



Scenario 1: Project progress passes Midterm Review.

Scenario 2: Project does not pass Midterm Review. End of project.

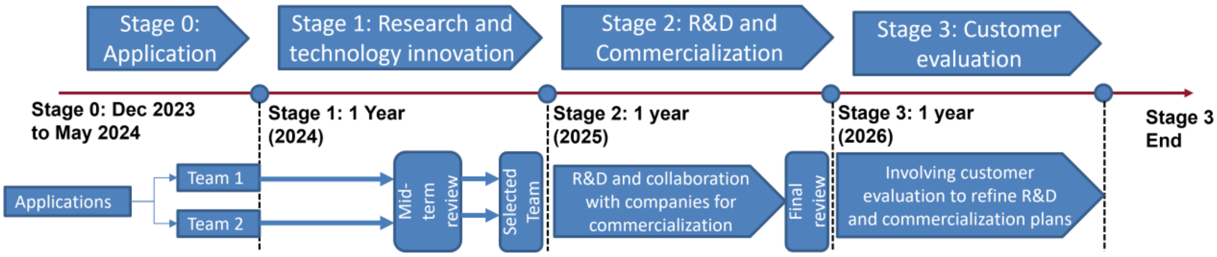
8.9. If the team passes the interim term Review, funding support for the team to continue the research project will be made available. CRPO reserves the rights to terminate, after interim term Review or at any point in time, a project that does not meet the minimum expectations of progress and achievement, upon recommendation by the Evaluation Committee.


Scenario 1: Project progress passes Interim Review.
Scenario 2: Project does not pass Interim Review. End of project.

8.10. The Evaluation Committee may also make recommendations to maximise the outcomes of funded projects which include, but are not limited to, adjustments to proposed durations, and qualifying only certain components of a project to proceed to completion.

8.11. Teams will be required to give a presentation after the end of term for final assessment.

8.12. An illustration of the grant review and project performance assessment is shown below:


Stage 0: Application
Stage 1: Research and technology innovation
Stage 2: R&D and Commercialization
Stage 3: Customer evaluation
Stage 0: Dec 2023 to May 2024
Stage 1: 1 Year (2024)
Stage 2: 1 year (2025)
Stage 3: 1 year (2026)
Stage 3 End
Applications
Team 1
Team 2
Mid-term review
Selected Team
R&D and collaboration with companies for commercialization
Final review
Involving customer evaluation to refine R&D and commercialization plans

9. Application

9.1. All applicants must fully comply with CRPO Grant Call Rules and Guidelines, Annex B – Terms and Conditions of CRPO Grant and Annex C - Guidelines for the Management of CRPO Grant, which can be downloaded from www.ntu.edu.sg/crpo.

9.2. Interested applicants should submit the CRPO Grant Application Form and other supporting documents in PDF (and Word if applicable). All applications must be submitted through the Host Institution via email to CRPO@ntu.edu.sg according to the timeline specified in paragraph 6.7.

9.3. Only complete application with the endorsement of the relevant institutional authority/director of research (or equivalent), will be accepted by CRPO.

9.4. Late submissions or submissions from individual applicants without the endorsement of the relevant institutional authority/director of research (or equivalent), will not be entertained.

10. Other Guidelines and Information

10.1. Proposal Content

10.1.1. The Proposal must adhere to the page limit, prescribed format and address the points as stated in Annex A-Proposal Template for CRPO Grant Call.

10.1.2. When applicable, a letter of support from the industry partner(s) is required. Commitment by the industry partner to provide the relevant proprietary datasets, a portion of project costs in cash and in kind will be viewed favourably.

10.1.3. Letter of support is required from the end customer for the deployment or end usage of the solution or the industry partner on the translation plan and deployment.

10.1.4. 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.

10.2. Intellectual Property

10.2.1. Intellectual Property ("IP") developed under the grant call ("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. The IP arrangement is "Soley Developed Soley Owned and Jointly Developed Jointly Owned".

10.2.2. The Institutions shall keep and maintain a fully comprehensive and updated list of all such Research IP and make such details available to CRPO and/or the grantors for inspection at any time.

10.2.3. The Institutions shall grant CRPO a non-exclusive, non-transferable, sub-licensable, perpetual, irrevocable, worldwide, royalty-free right and license to use, modify, reproduce and distribute the Research IP for research, development and/or commercial purposes (The "CRPO License").

10.2.4. Except the rights expressly licensed or otherwise provided in this Rules and Guidelines or Annex B – Terms and Conditions of CRPO Grant, 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 CRPO.

10.2.5. Management of all Research IP shall have reference to and be guided by the Public Sector Master Research Collaboration Agreement (PS MRCA) and key principles of the Singapore National IP Protocol for Publicly Funded R&D. In general, Research IP may be open-sourced for research and experimentation and licensed for commercial deployment.

10.2.6. 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 CRPO, the Institutions shall attend such meetings as CRPO may direct to discuss the potential for exploitation and commercialisation of Research IP.

10.2.7. The Institutions shall reserve a royalty-free, irrevocable, worldwide, perpetual and non-exclusive right for the Singapore Government and public sector agencies to Research IP for their statutory functions, non-commercial and R&D purposes.

10.2.8. The IP terms in Clause 10.2 of this Rules and Guidelines are deemed to be incorporated into the Terms & Conditions of CRPO Grant (Annex B).

10.3. Ethics and Confidentiality

10.3.1. All the Investigators, Collaborators, staff, and students working on the project must comply with the relevant local laws or regulations governing the research.

10.3.2. 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.

10.3.3. 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.

10.3.4. The work should be conducted under strict international, national, and/or institutional guidelines on privacy and confidentiality protection of personal data use.

10.3.5. 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.

10.3.6. 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.

10.4. Project Support and Facilitation

10.5. CRPO is equipped with common research-engineering capabilities to facilitate or support the Cyber Security community. With respect to the grant call, the potential resources that applicants may leverage include:

10.5.1. **iTrust Testbeds:** iTrust is the proud host of several world-class testbeds and lablets. These testbeds and lablets together constitute a one-of-a kind facility for research and training in the design of safe and secure large-scale cyber physical systems. The testbeds aid in the design and testing of devices that fall under the Internet of Things. The lablets support training programs in the area of Cyber Physical Systems. The following testbeds and lablets are available to researchers at iTrust and its partners across the world. You can find more information here: https://itrust.sutd.edu.sg/testbeds/

10.5.2. **NCL Tesbeds:** National Cybersecurity R&D Lab (NCL), established in 2015 and funded under the National Cybersecurity R&D (NCR) Programme. NCL aim is to provide support to the Singapore cybersecurity R&D community in terms of their research experimentation and testing requirements. NCL offers computing resources and controlled experimentation environments to facilitate collaborative research among academia, government bodies, and industry. The infrastructure comprises a cluster of 300+ nodes with diverse provisioning mechanisms, security data, and security services. OpenStack, an open-source cloud computing infrastructure software project, serves as the foundation for managing the NCL infrastructure. In addition to Compute and Baremetal, NCL also supplies a range of GPU servers to accommodate the growing requirements of AI research. You can find more information here: https://ncl.sg/

10.5.3. **NICE Facility:** National Integrated Centre for Evaluation (NiCE) @ NTU is a collaboration between Cyber Security Agency of Singapore (CSA) and NTU. Strategically located in NTU to leverage on their knowledge, expertise and experience in software and hardware assurance, NiCE will be a one-stop facility for product testing, inspection and evaluation. You can find more information here: https://www.ntu.edu.sg/nice

10.5.4. Facilitating Cyber Security Collaborations and Innovation

10.5.5. **Industry Connections and Matchmaking:** In our pursuit of advancing cybersecurity, CRPO endeavors to bridge the gap between industry and innovators. We actively collect, curate, and regularly update a comprehensive repository of the skillsets, needs, and interests within the Cyber Security industry. This valuable information is readily accessible on our website, empowering interested applicants to explore potential partnerships seamlessly. Whether you're seeking a collaboration or looking for a specific skillset, our platform acts as a dynamic hub for industry matchmaking.

10.5.6. **System Engineering and Rapid Prototyping:** At the heart of CRPO's capabilities lies a versatile engineering pool equipped with expertise in software and network engineering, web services, privacy-preserving applications, and AI/ML. This dedicated team, comprising the CRPO, stands ready to contribute to project prototyping and Proof of Concept (PoC) development. Leverage the collective skillset of CRPO's engineering talent to fast-track your project from conceptualization to tangible results, ensuring efficiency and innovation.

10.5.7. **Guidance on Translational Opportunities:** Entrepreneurs, researchers, and visionaries are encouraged to engage with CRPO in a dynamic exchange of ideas. We extend an open invitation for applicants to connect with us, seeking advice and insights on the translational efforts related to their cybersecurity concepts. Our experts are available to address queries, provide guidance, and share valuable perspectives on navigating the landscape of translational endeavors. Unlock the potential of your ideas with CRPO's collaborative and supportive ecosystem.

10.5.8. In essence, CRPO serves as a catalyst for synergy within the Cyber Security realm, offering a platform where industry needs meet innovative solutions. From industry matchmaking to hands-on project support and insightful guidance, CRPO is committed to propelling the field forward through collaboration and knowledge exchange. Connect with us and embark on a journey of transformative cybersecurity innovation.

10.6. Alignment with CRPO's Research Focus:

10.6.1. Requests for resources detailed in paragraph 10.5 should align seamlessly with the current research focus of CRPO. It is imperative that applicants, in their proposals, clearly articulate how their resource needs directly contribute to and complement the ongoing research priorities of CRPO. This alignment is pivotal in ensuring that the resources requested contribute meaningfully to the advancement of our collective research objectives.

10.6.2. **Quantification of Resource Needs:** Applicants are expected to provide a clear and quantifiable assessment of their resource requirements within their proposals. This includes specifying the type and quantity of resources needed from CRPO to facilitate their research endeavors. This information will be critically evaluated as an integral part of the proposal request process, aiding in the efficient allocation of resources.

10.6.3. **Justification for Resource Requests:** Recognizing the constraints of limited resources, applicants must provide compelling justifications for their resource requests. The onus is on the applicants to elucidate how the requested resources align with the objectives of their research and why they are integral to the success of their projects. CRPO reserves the right to evaluate and, if necessary, turn down requests that do not meet the criteria of strategic alignment and justification.

10.6.4. **Cost Implications and Facilities:** Applicants should be mindful of the specific costs associated with the facilities mentioned in paragraph 10.5. Clearly outlining the budgetary requirements in their proposals will enhance the transparency of resource needs. This ensures that both CRPO and the applicants have a comprehensive understanding of the financial implications involved.

10.6.5. **Availability Considerations:** It is important to note that, due to various factors, some of the resources listed may not be immediately available. Applicants should be prepared to incorporate flexibility into their timelines, understanding that certain resources may require additional lead time for procurement or allocation.

10.6.6. In summary, CRPO values the strategic alignment, quantification, and justification of resource requests within the context of our research priorities. We encourage applicants to thoroughly assess their needs, articulate them clearly in their proposals, and engage in a collaborative dialogue with CRPO to optimize the utilization of available resources.

11. Contact Information

11.1. For any enquiries, please contact CRPO@ntu.edu.sg