Cybersecurity

Co-Innovation and Development Funding (CCDF)

2025

Information Kit

Release Date: 14 Nov 2025

CYBERSECURITY CO-INNOVATION AND DEVELOPMENT FUNDING (CCDF) INFORMATION KIT

1. BACKGROUND

1.1. As cyber-attacks become increasingly sophisticated, the cybersecurity industry faces continuous pressure to keep pace with the rapid evolution of threats. Innovation plays a crucial role in enabling governments and organizations to stay ahead in the ongoing "arms race" against cyber attackers.

1.2. The Cyber Security Agency of Singapore ("CSA") has developed the Cybersecurity Co-innovation and Development Fund (CCDF) to catalyse the development of innovative cybersecurity solutions for national security, strategic applications, and commercial purposes.

1.3. The objective of the CCDF is to foster the development of advanced solutions, technologies, and approaches that enhance cybersecurity measures. CCDF aims to tackle emerging threats, vulnerabilities, and challenges in the digital landscape by promoting creativity and ingenuity in the field of cybersecurity. By driving innovation, the industry aims to proactively address cyber threats, safeguard sensitive information, and ensure the privacy and safety of individuals, organizations, and critical infrastructures.

1.4. CCDF also aims to contribute to industry growth by encouraging research and development, addressing emerging threats, promoting collaboration, enhancing competitiveness, and meeting evolving customer needs.

2. SCOPE

2.1 We are looking for solutions in the following areas, but not limited to:

a. **Cybersecurity for Artificial intelligence (AI)**
Safeguarding AI systems and the data they process from various cyber adversarial attacks in order to maintain the integrity, confidentiality, trustworthiness and reliability of AI applications in an increasingly connected and digital world.

b. **Artificial intelligence (AI) for Cybersecurity**
Harnessing the power of AI to strengthen cyber defences, improve threat detection, and respond more effectively to the evolving and sophisticated nature of cyber threats, thereby helping organisations protect their systems, data and networks from cyber-attacks.

c. **Quantum Safe**
Protecting critical digital systems, data, and infrastructure from the potential threat of Cryptographically Relevant Quantum Computers by transitioning to quantum-resistant solutions and enabling cryptographic agility and defense-in-depth.

d. **Operational Technology (OT) / Internet of Things (IoT) Security**
Safeguarding critical infrastructure, Industrial Control Systems (ICS) and internet-connected devices from cyber threats and vulnerabilities.

e. **Cloud Security**
Safeguarding data, applications, resources and infrastructure hosted in cloud environments, while maintaining the confidentiality, integrity and availability of resources in the cloud.

f. **Privacy-Enhancing Technologies (PET)**
Safeguarding the privacy of individuals and confidentiality of their data while using systems and digital services, thereby empowering individuals to manage their data securely and complying with privacy regulations.

3. ELIGIBILITY

3.1. All companies registered in Singapore are eligible to apply for funding under the CCDF. Overseas firms not registered in Singapore must partner with a registered Singapore company, which must hold the foreground Intellectual Property (IP) of the development.

3.2. Companies must ensure that at least 50% of the funded workforce involved in the project are Singapore residents or possess Singapore Permanent Residency (PR). All funded personnel must physically work in Singapore.

3.3. Companies are expected to have adequate financing resources to ensure that they have the ability to see through the completion of the project.

3.4. For proposals submitted under the Open Category, applicants must secure at least one committed cybersecurity end-user by the third milestone of the project. The proposed cybersecurity end-user must be approved by CSA.

3.5. Companies can leverage "minimum viable products" and/or market-ready technologies to develop cybersecurity applications with new features and functionalities that meet the emerging demands of cybersecurity users.

3.6. Projects that work solely on system integration and customization will not be funded.

3.7. Retrospective applications will not be accepted. An application is considered retrospective if the proposed project has already commenced before/at the time of application.

4. FUNDING SUPPORT

4.1. Each project funded under the CCDF can receive up to S$1,000,000 for a period of up to 24 months. The funding covers potentially the expenditure related to manpower, professional services, equipment, and/or software required for the development of the innovative product/solution.

4.2. The funding awarded must be utilized for development activities in Singapore unless otherwise approved. Recipients of funding must register, own, and manage all intellectual property rights arising from the project in Singapore.

4.3. Proposals already funded or under consideration for funding by other government agencies will not be considered under the CCDF.

5. EVALUATION PROCESS

5.1. Proposals received by the Secretariat will undergo assessment by a team of evaluation panel. Shortlisted applicants will be invited to present their proposals to the evaluation panel.

5.2. Proposals will be evaluated based on the following criteria:

a. **Quality and Innovation**
The solution must demonstrate innovation and uniqueness. It should not be a system integration of existing products. The problem should be tackled with a creative strategy rather than a purely technical or engineering method.

b. **Applicability Beyond Current End-user**
The solution should address not just the immediate needs of a single entity but also hold the capacity for broader implementation across the industry. It should be applicable to other organizations facing similar challenges. The submission should include a business strategy for the 1 to 2 years following project completion, detailing plans to broaden the solution's uptake among a more extensive clientele.

c. **Competency of Project Team**
The project team should possess the necessary expertise and a track record of delivering successful projects related to the proposed technologies. The company should have adequate financial resources to ensure the project's progress to its full fruition.

5.3. The shortlisted applicants and the proposed funding percentage/value will be determined based on the assessment conducted by the evaluation panel. The decision of the evaluation panel is considered final.

6. SUBMISSION PROCESS

6.1. To apply for the CCDF, please visit:

https://www.csa.gov.sg/our-programmes/innovation-schemes/csa-cybersecurity-co-innovation-and-development-fund/

7. RESULTS AND ACCEPTANCE OF AWARD

7.1. Only successful applicants will be informed of the results of their application.

7.2. The offer of the award under the CCDF will be sent to the successful applicant through a Letter of Offer. The Letter of Acceptance with the terms and conditions of the award, must be duly signed by the applicant, and reach the Secretariat within 14 working days from the date of the Letter of Offer.

8. CLAIMS

8.1. All claims will be disbursed on a reimbursement basis upon the submission of the progress report with its supporting documents such as payslips and invoices, and upon approval by the secretariat.

8.2. Disbursement will take place in tranches in accordance with the defined milestones committed in the project timeline.

8.3. The claim for the last milestone must be accompanied with an audited report on the total costs claimed by the company. The cost of audit will be borne by the company.

9. CONTACTS

9.1. For more information on the CCDF, please contact CCDF Secretariat at CyberCall@csa.gov.sg