Cyber Cooperation Program Open Grants Process
Applicant Guidelines

Contents

Section 1: Context .............................................................................................................................. 2
Geographic Focus .......................................................................................................................... 3

Section 2: Operational Objectives ................................................................................................. 3
Cyber Security in Critical Sectors.................................................................................................. 4
Human Rights and Democracy Online ......................................................................................... 4
Mainstreaming Gender Equality and Women’s Empowerment within Cyber Affairs .................. 5
Theory of Change .......................................................................................................................... 5

Section 3: Selection Criteria .......................................................................................................... 6
Proposed Budget and Project Duration .......................................................................................... 8

Section 4: Application Process ...................................................................................................... 8
Deadline ....................................................................................................................................... 8
Indicative timeline ......................................................................................................................... 9
Applicant Briefing .......................................................................................................................... 9
Conformance Check ....................................................................................................................... 9
Selection Process ........................................................................................................................... 9
Debriefing Applicants .................................................................................................................... 10
Complaints .................................................................................................................................... 10

Section 5: Assessment of Grant Proposals .................................................................................... 10

Section 6: Social Safeguards and Risk Management ...................................................................... 10
Child Protection ............................................................................................................................ 10
Safeguards, Inclusion Policies and Risk Management .................................................................. 11

Section 7: Contractual, Reporting and Acquittal Requirements ..................................................... 11

Section 8: Contact .......................................................................................................................... 11
The Cyber Cooperation Program (the Program) Open Grants process seeks to explore and test new, innovative approaches to achieving Program outcomes, partnering with new implementing partners or working in new sectors. This may include supporting research that builds understanding of cyber issues, challenges and opportunities. The Open Grants process is available to Australian and non-Australian academic institutions, non-government organisations, regional and multilateral organisations and the private sector.

DFAT will manage the administration of the process and outcomes, as well as the direction and selection of activities.

**Section 1: Context**

Australia's former Foreign Minister, The Hon Julie Bishop MP, launched Australia's first International Cyber Engagement Strategy (the Strategy) on 4 October 2017 in Sydney. The Strategy is global in perspective and regional in focus, championing an open, free and secure Internet that protects national security and promotes international stability, while driving global economic growth and sustainable development.

The global Internet and digital technologies are profound enablers of sustainable development and inclusive economic growth. The United Nations 2030 Agenda for Sustainable Development recognises digital technologies as vital to ending poverty, expanding access to quality education, achieving gender equality and social inclusion, promoting inclusive economic growth, improving health outcomes and supporting cross-sectoral innovation.

The spread of digital technologies increases profound economic opportunities but, at the same time, creates new vulnerabilities. Individuals, the private sector and governments around the world face an evolving array of cyber threats. An open, free, and secure cyberspace is essential to fully realising the benefits of these new technologies.

The global nature of cyberspace means Australia must engage internationally to advance and protect our shared interests in cyberspace. The Program provides the framework to partner with countries in the Indo-Pacific region to ensure they are equipped to take advantage of opportunities presented by an open, free and secure cyberspace as well as respond to new cyber challenges. Projects funded by the Program aim to improve cyber resilience across the full spectrum of cyber affairs – including enhancing cyber security, building cybercrime capacity, promoting respect for human rights and democratic principles online and encouraging the use of digital technologies to achieve sustainable development.

The success of the Program is based on its strong partnerships model, which sees industry, academia, civil society, Australian Government agencies and other like-minded donors partner with countries across the Indo-Pacific to combine knowledge and resources to advance and protect our collective interests in cyberspace.

The private sector plays a crucial role in enabling access to the Internet and contributing to discussions on the policy and technical management of the Internet through a multi-stakeholder approach. The Program will continue to partner with the private sector, leveraging their expertise, resources and relationships to achieve Program outcomes.
**Geographic Focus**

Indo-Pacific countries recognise the importance of the Internet to their future economic growth and prosperity and are increasingly aware of the need to address the associated challenges. They are reaching out to Australia, other donors, institutions, multilateral partners and non-government organisations to help develop and strengthen their institutional capacity to respond to new threats, vulnerabilities and risks; understand their obligations online; respect and protect individual rights; as well as making best use of the Internet to drive economic growth, protect national security and promote international stability.

The ASEAN and Pacific regions are highly diverse, comprising developed, emerging and developing economies, each at a different point in their digital journey. Many Indo-Pacific countries are global leaders, at the forefront of production and global exportation of new technologies, with expanding digital economies, established cyber security industries and mature cyber policy and governance structures.

However, the Indo-Pacific is also home to some of the world's least connected countries, with limited Internet penetration and digital opportunities yet to be fully harnessed. These challenges are particularly acute for Pacific island countries. The Pacific Island Forum Leaders Boe Declaration, endorsed in September 2018, highlighted cyber security as an emerging security challenge for the region and recognised the need to maximise the protections and opportunities for Pacific infrastructure and societies in the digital age.

**Section 2: Operational Objectives**

Within the relevant geographic area, project proposals must align with the objectives and desired end-of-program outcomes of the Program.

Focusing on areas of highest demand from our regional neighbours, the five priority intermediate outcomes of the Program are:

1. An international cyber stability framework which promotes responsible state behaviour in cyberspace;
2. Stronger cybercrime prevention, prosecution and cooperation;
3. Building cyber security capability for a strong and resilient cyber security posture;
4. Best practice use of technology to support economic growth and sustainable development; and
5. Advocating and protecting human rights and democracy online.

The End of Program outcome is:

*Selected states in ASEAN and the Pacific region increase awareness, commitment, action and international engagement to strengthen cyber resilience and build sustainable partnerships with Australia by 2023.*
This Open Grants process will consider proposals under all five intermediate outcomes, but will prioritise proposals that focus on the following areas:

1. Building cyber security and incident response capability for a strong and resilient cyber security posture within critical sectors;
2. Advocating and protecting human rights and democracy online; and
3. Mainstreaming gender equality within cyber affairs.

The Program has a specific geographic focus on ASEAN states and Pacific island countries. Activities are focused at the bilateral level (Indonesia, Solomon Islands, Vanuatu, Fiji, Tonga, Papua New Guinea, Samoa) and regionally (ASEAN and Pacific) to reflect Australia’s broader strategic policy interests and where we can best leverage our resources to maximise development impact. While the above-mentioned countries are prioritised, the Open Grants process will consider proposals for other ASEAN or Pacific country eligible for Official Development Assistance (ODA).

**Cyber Security in Critical Sectors**

Effective cybersecurity is key to harnessing the economic potential of the digital revolution. Engaging internationally to strengthen the collective cyber security of Australia, the Indo-Pacific and the broader global community – given the global nature of the Internet – is in all our interests.

The Program seeks to identify opportunities to mature the national cyber security and incident response capability and posture of the Program’s priority countries. The Open Grants process seeks project proposals focused on critical infrastructure sectors, such as (but not limited to): banking and finance; water and energy; transport (e.g. aviation) and communications.

Proposed activities could range from awareness raising; mentoring and support in developing governance frameworks; technical training; threat intelligence and information sharing; collaboration mechanisms; and other best practice and innovative solutions.

**Human Rights and Democracy Online**

The universal protection and promotion of human rights and democratic principles online is vital to achieve lasting peace, security, freedom and dignity for all. Australia firmly believes that human rights apply online as they do offline.

The Program is working to establish and strengthen national frameworks that respect and protect human rights and democracy online. It is expected that through the Program, Australia will work with countries to increase their capacity to respond to and manage issues associated with harmful content online in a manner consistent with human rights and democratic principles.

Proposed activities could cover the following themes:

- Advocate and ensure respect for the protection of human rights and democratic principles online;
- Explore the linkages between human rights, technology and/or cyber security; and
- Increase capacity to respond to and manage harmful online content in support of human rights.
Mainstreaming Gender Equality and Women’s Empowerment within Cyber Affairs

Development of an open, free and secure Internet in the Indo-Pacific region supports gender equality and women’s empowerment. The Program advocates for gender equality and women’s empowerment principles to be applied to all activities and at all relevant stages in the project management cycle. This will ensure that gender equality is actively pursued in activities supported through the Program and that professionalisation of a global cyber workforce promotes technical and leadership opportunities for women.

The Open Grants Process seeks project proposals that support greater awareness and understanding of how gender and women’s empowerment issues can be impacted by greater connectivity.

Proposed activities could cover the following themes:

• Seek to increase women’s meaningful access to the Internet;
• Encourage women’s participation in policy making and reform; and
• Explore the linkages between human rights, women and cyberspace, for example in relation to violence towards women online.

Theory of Change

The Program has a basic theory of change that focuses on improving human capital and capability to address cyber challenges within the region.

DFAT has identified its most successful strategies for generating institutional change as:

• taking an incremental rather than comprehensive approach to improving existing capacities and functions;
• seeking flexible, localised, fit for purpose solutions rather than relying on institutional templates; and
• focusing on issues where there are local constituencies for change that could be mobilised and supported, for example local providers who can assume ownership once a project is complete.

Applicants should ensure their project proposals are guided by the following principles underpinning the Program:

• Context matters: The Program takes into account the political, economic and socio-cultural contexts across the various countries and regions in order to provide tailored solutions. It adds value to existing initiatives and works collaboratively with other Australian-funded initiatives, and with like-minded organisations and governments to achieve outcomes.

• Multi-stakeholder approach: The Program advocates for a multi-stakeholder approach to internet governance that is inclusive, consensus-based, transparent and accountable in recognition that all stakeholders have valuable contributions to make.

• Gender equality: The Program advocates for gender equality and women’s empowerment principles to be applied to all activities and at all relevant stages in the project management cycle. This ensures that gender equality is actively pursued in activities supported through the Program and that professionalisation of a global cyber workforce promotes technical and leadership opportunities for women.

• **Sustainability:** The Program promotes lasting impact through approaches that promote counterpart ownership. By working through core delivery partners, it encourages the use of local, private sector and other non-ODA funding to broaden stakeholder buy-in and support for outcomes. Similarly, it uses local systems and processes as a means to strengthen local institutions as a basis for ongoing country-led delivery.

• **Change through diplomacy:** Long-term relationships between Australian and counterpart governments build confidence that will endure beyond the individuals involved in the Program today. The Program informs and sensitises people and governments to the benefits of an open, free and secure Internet, through evidence, technical assistance and influence.

• **Embracing innovation:** Innovation is a critical factor in sustaining an open, free and secure cyberspace. Innovators develop new ways for people to participate and collaborate online. This ensures that cyberspace remains an ever-evolving force for inclusive economic growth and sustainable development. The Program tests and pilots new ideas for achieving outcomes, introducing new and affordable technological platforms, being willing to learn from successes and failures, and bringing successes to scale through support for replication.

### Section 3: Selection Criteria

Project proposals will be assessed against the following criteria:

• **Criteria 1:** Does the proposal pursue Australia’s national interest?
  Consider whether the proposal aligns with relevant strategy documents such as Australia’s aid strategy, the International Cyber Engagement Strategy, Australia’s Cyber Security Strategy.

• **Criteria 2:** Does the proposal have a positive impact on promoting growth and reducing poverty?
  Consider whether the proposal aligns with relevant Aid Investment Plans, other aid investments, objectives of the Cyber Cooperation Program, advances a host government priority and has their support.

• **Criteria 3:** Does the proposal take advantage of Australia’s value-add and leverage?
  Consider whether the proposal best leverages Australia’s capabilities, engages the private sector and leverages host government resources.

• **Criteria 4:** Is the proposal value-for-money and focused on results?
  Consider how the proposal contributes to one or more of the following strategic targets of the aid program: can deliver on commitments, works with the most effective partners, ensures value for money, increases consolidation and empowers women and girls.
Project proposals will be scored according to the below scale:

<table>
<thead>
<tr>
<th>Score</th>
<th>Rating Scale</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td><strong>Very Good:</strong> Satisfies criteria in all areas. The activity is sound and represents low risk.</td>
</tr>
<tr>
<td>4</td>
<td><strong>Good:</strong> Satisfies criteria is almost all areas. The activity is workable and well substantiated in key areas. The activity is low risk and any residual risks can be managed.</td>
</tr>
<tr>
<td>3</td>
<td><strong>Adequate:</strong> on balance satisfies criteria; does not fail in any major area. The solution is plausible but some shortcomings and/or deficiencies could give rise to a lack of complete satisfaction.</td>
</tr>
<tr>
<td>2</td>
<td><strong>Less than adequate:</strong> on balance does not satisfy criteria and/or fails in at least one major area. The solution is medium/high risk.</td>
</tr>
<tr>
<td>1</td>
<td><strong>Poor:</strong> Does not satisfy criteria in all/most areas. The solution is unworkable with a high probability of failure. The solution is high risk.</td>
</tr>
</tbody>
</table>

Proposals must attach letters of support from two referees. These should address the Organisation’s experience and capacity to achieve the objectives of the Program.

An Organisation’s Certification must be completed in SmartyGrants.

The Program will not support project proposals:

- without strong potential to have a positive impact on cyber resilience in the identified countries/region;
- that duplicate current programs and projects;
- that include salary replacement or supplementation for in-country partners; or
- that involve social research of a primarily investigative nature (certain operational or implementation research activities may be considered where there is judged to be strong potential for policy and/or human resource development impacts).

Individuals with conflicting commitments and current and recent DFAT employees (see below) must not be included in the project proposal or as individuals who may be engaged if selected through the assessment process. DFAT may reject any project proposal that does not disclose that a proposed team member has an existing and continuing commitment to another DFAT program or project. Project proposals compiled with the assistance of current or recent DFAT employees will be excluded from assessment.

Recent DFAT employees are those whose employment ceased within the nine months prior to the submission of the project proposal and who were substantially involved in the design, preparation, appraisal and/or review of this or substantially related programs.

Applicants must ensure that proposals meet all eligibility requirements at the time of submission and for the duration of the period of assessment and review.
Proposed Budget and Project Duration

Depending on the project scope and size of the applicant’s organisation, consideration will be given to provide funding of up to $500 000 over two years. Actual duration and funding levels will be determined by the Evaluation Committee in consultation with successful applicants.

The indicative budget may include the following costs:

- **Personnel** - Proposed salaries for each member of the team and/or associated staff should be based on operational requirements.

- **Capacity development activities** – Costs of capacity development activities in these areas can include specialised training, mentoring, seminars and workshops.

- **Fieldwork** – In-country fieldwork expenses, including costs associated with establishing the project in-country.

- **Travel** – Costs for domestic and/or international economy class airfares and modest accommodation and per diems that are essential for delivery of the project.

- **Equipment** – DFAT will only fund ‘small equipment’ or software specific to the project proposal. ‘Small equipment’ is defined as equipment under a total of $10,000 that is used collaboratively and, where possible, is Australian-made. Computing equipment or software should be specialised and required for the completion of the project. DFAT will not fund general equipment or software that would be normally provided by institutions, such as standard computers or the Microsoft software suite.

- **Monitoring, evaluation and learning (MEL)** – As a key component of the program, costs associated with MEL processes and activities to inform program reporting and learning should be identified separately within the indicative budget outline.

- **Administrative support**

- **Other associated costs** – Budget items that cannot be appropriately placed in other categories.

Section 4: Application Process

**Deadline**

Completed project proposals, with supporting documents, should be submitted through SmartyGrants no later than 5pm Australian Eastern Daylight Time (AEDT) on 14 February 2020. Late applications will not be accepted.
Indicative timeline

1. The indicative timeline for this Open Grants process is summarised below:

<table>
<thead>
<tr>
<th>Event</th>
<th>Date Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applications open</td>
<td>17 January 2020</td>
</tr>
<tr>
<td>Applications close</td>
<td>14 February 2020</td>
</tr>
<tr>
<td>Assessment of proposals by DFAT in</td>
<td>17 February – 6 March 2020</td>
</tr>
<tr>
<td>consultation with Australian Government</td>
<td></td>
</tr>
<tr>
<td>partners</td>
<td></td>
</tr>
<tr>
<td>Evaluation Committee to agree shortlisted</td>
<td>9 – 13 March 2020</td>
</tr>
<tr>
<td>proposals</td>
<td></td>
</tr>
<tr>
<td>DFAT makes offer(s) to preferred applicant(s)</td>
<td>16 – 20 March 2020</td>
</tr>
<tr>
<td>Negotiation of Grant Agreements, including</td>
<td>23 March – 17 April 2020</td>
</tr>
<tr>
<td>due diligence assessments</td>
<td></td>
</tr>
<tr>
<td>Payment of first tranches of funding</td>
<td>End May 2020</td>
</tr>
<tr>
<td>Program implementation commences</td>
<td>End May 2020</td>
</tr>
</tbody>
</table>

Applicant Briefing

DFAT will not hold an applicant briefing under this Open Grants process. Applicants are encouraged to check the Business Opportunities page on the DFAT website for all documentation related to the program and invitation. Questions requiring clarification should be sent by email to the Program contact (refer Section 8 below). All questions and answers and any resulting addenda to these Guidelines will be published on the DFAT website so that all organisations have equal access to information.

Conformance Check

Activity Proposals will be checked by DFAT for conformity in terms of the requirements set out in these Guidelines and the form on SmartyGrants. At the discretion of DFAT, those proposals deemed non-conforming will be excluded from assessment and applicants will be advised by DFAT.

Selection Process

DFAT will establish an Evaluation Committee to assess and rank conforming applications against the selection criteria. The committee will include members with appropriate expertise to:

a. review applications against the selection criteria
b. review budgets to ensure value for money
c. score applications to produce a ranked list of applications with recommendations for funding to provide to DFAT.
The panel is conducted on a confidential basis and panel members are required not to discuss matters relating to the assessment of any proposal with any external party. Applicants must not seek contact with any members of the panel, and any such contact will be considered a breach of confidentiality and may result in DFAT rejecting the proposal of the applicant concerned.

**Debriefing Applicants**

Applicants are entitled to request a written debriefing on the results of the assessment of their proposals once a Grant Agreement has been signed with the successful applicants. This debriefing will provide information on scores achieved against selection criteria. DFAT will not enter into discussion or communication on the content of the debrief once it has been issued.

**Complaints**


**Section 5: Assessment of Grant Proposals**

In making final funding decisions, DFAT may consider additional factors relevant to the suitability, capacity and qualifications of an applicant, including but not limited to:

  a. checking with other persons or organisations on the accuracy of information and quality of previous work performed, including the resourcing of previous work (past performance information); and  
  b. information obtained from any legitimate, verifiable source which is relevant to the capacity of the applicants.

Such information will be raised with the applicant if needed.

On receipt of the Evaluation Committee’s recommendations, the DFAT delegate will make final decisions on which proposals to fund and to what value. In making final decisions, DFAT reserves the right to ensure an appropriate balance of investments across the relevant geographical areas in the Indo-Pacific region.

**Section 6: Social Safeguards and Risk Management**

DFAT Safeguards for the Australian aid program apply to environmental protection, displacement and resettlement, and child protection. Implementing Partners are required to adhere and apply these safeguards throughout the life of the Program. Implementing Partners should refer to DFAT’s Environmental and Social Safeguards on the DFAT website for the most up to date versions of DFAT Safeguards.

**Child Protection**

The Program will apply the DFAT Child Protection Policy and Preventing Sexual Exploitation, Abuse and Harassment Policy. Originally released in January 2013 and updated in January 2017, the Policy applies to all Implementing Partners and any sub-contractors who are using DFAT funds. DFAT’s Policy sets out standards that provide a framework for managing and reducing the risks of child exploitation and abuse. The Policy recognises the shared and
collective responsibility of all adults to prevent child exploitation and abuse and DFAT’s own responsibilities as the Australian Government’s lead overseas aid agency, to working with its partners to prevent and respond to child exploitation and abuse. It further recognises that child sex offenders often seek employment or volunteer placements in organisations that work with children in Australia or overseas in order to access vulnerable children. Therefore the policy is designed to protect children across the world from (or from further) exploitation and abuse and sexual, physical and psychological violation. The Policy takes a risk-based approach to Child Protection, requiring active engagement with Child Protection at all levels of the organisation and program to identify, mitigate, manage and reduce the risks to children. The goal of the Policy is to protect children from exploitation and abuse of all kinds in the delivery of Australia’s overseas aid program.

The Program is obliged, under DFAT’s Child Protection Policy, to have a DFAT-compliant Child Protection Policy. Any activities by Implementing Partners that may have contact with, or impact on children must apply the Minimum Child Protection Standards and should seek to build upon these standards where possible. All DFAT funded partners working with, or having contact with children, must also adhere to the Child Protection Professional Behaviours while undertaking business on behalf of DFAT.

**Safeguards, Inclusion Policies and Risk Management**

Further information on DFAT’s gender equality and disability inclusion policies and approaches is available online:


Further information on safeguards and DFAT’s approach to risk management is available at:


**Section 7: Contractual, Reporting and Acquittal Requirements**

Successful applicants will be engaged under a Grant Agreement with DFAT that will detail agreed implementation, accountability, funding, reporting and acquittal requirements. DFAT may request applicants amend parts of their proposals, such as project plans or risk management approaches, during this process.

A template of the Grant Agreement is included with the Program documents.

**Section 8: Contact**

Enquiries in relation to the Open Grants process should be directed to [CyberAffairs@dfat.gov.au](mailto:CyberAffairs@dfat.gov.au) no later than 1700 Australian Eastern Daylight Time (AEDT) on 31 January 2020. DFAT will not respond to any enquiries submitted after this date.

All enquiries, replies and associated addenda (where required) will be posted on the Business Opportunities page of the DFAT website.