**FCO International Cyber Security Capacity Building Fund Criteria**

The FCO’s International Cyber Security Capacity Building Fund was launched by the Foreign Secretary at the Budapest Cyber Conference on 4-5 October 2012. The initiative forms part of the Cabinet Office-led National Cyber Security Programme (NCSP), which runs until 2015.

The FCO International Cyber Capacity Building Fund is intended to bolster international capacity building linked to supporting the vision of the UK National Cyber Security Strategy:

*for the UK in 2015 to derive huge economic and social value from a vibrant, resilient and secure cyberspace, where our actions, guided by our core values of liberty, fairness, transparency and the rule of law, enhance prosperity, national security and a strong society.*

The full strategy and objectives can be found [here](http://www.cabinetoffice.gov.uk/resource-library/cyber-security-strategy).

**Focus of the FCO International Cyber Security Capacity Building Programme**

**Financial Year 2014 - 2015**

**1. The focus of the fund is to support delivery of the National Cyber Security Strategy objectives**. Proposals should therefore make clear their potential measurable impact on the achievement of these objectives. The fund aims particularly to build capacity against the following categories as defined by the attached taxonomy:

1. National Cyber Security Strategies
2. Cyber crime
3. Security and resilience
4. International security
5. Governance, Economic Growth and social benefits

For an alternative structured definition of Cyber Security Capacity Building, see the Five Dimensions of the Oxford Global Cyber Security Capacity Centre at

<http://www.oxfordmartin.ox.ac.uk/cybersecurity/dimensions>

**2.** Bids are welcomed from governments, official bodies, businesses and NGOs where their influence can bring policy change or/ leading to demonstrable real world impact. Strong proposals will be high-impact interventions, defined by clear evidence of the potential to[[1]](#footnote-1):

1. Support NCSP objectives, ensuring UK and global security whilst protecting values and supporting an open internet AND/ OR substantially improving global co-ordination and effectiveness of Cyber Security Capacity Building.
2. Deliver solutions that are sustainable[[2]](#footnote-2) and/ or scalable[[3]](#footnote-3).
3. We also welcome bids which can demonstrate they can contribute effectively to wider International Development efforts.

**3. Proposals should outline clearly how the project complements the efforts of other partners** (non-governmental, developmental and private sector). Those proposing projects are expected to have investigated in-depth whether or not other similar projects already exist in the space. Projects which substantially overlap with other initiatives, or for which a more suitable funding source is available, will be rejected. Projects jointly funded by or delivered with other partners are welcomed as a way of increasing impact and enhancing co-ordination.

**4**. In the case of proposals from implementers which have already received FCO funds, **likely future delivery will be judged against past performance**.

**Accessing the fund/ Project Management Requirements**

**1.** Proposal forms are attached. These should be submitted in full, and in accordance with guidance provided. Incomplete proposal forms will not be reviewed by the Programme Board. If any aspect of the form requirements is unclear to applicants, we strongly recommend consultation with the Programme Team.

Language used should be clear and succinct.

Part A should include both qualitative and quantitative milestones. Details of beneficiary group participation and needs should include an explanation of how this will be measured and demonstrated.

Part B of the form should be completed by the FCO. Proposals should however include annexed evidence of:

* + previous experience delivering similar projects,
	+ strong assessment of any human rights risks associated with the proposed activities, and
	+ a clear statement of whether the implementer approves public reference to the project, with reasoning.

**2.** In addition to the requirements outlined above, proposals must provide details of how the project will be monitored. Monitoring methods should be robust, transparent, and include scope for beneficiary input. The methods identified should be designed to give a meaningful assessment of the project’s impact.

The FCO places a strong emphasis on evaluating projects, and all projects over £500,000 will be subject to a full, independent evaluation. Projects valued £100,000 and over may be evaluated.

**3.** Proposals must demonstrate a full assessment of project risks, with particular attention to any human rights implications of work carried out. Implementers should identify any risks which might apply to the project, what steps will be taken to mitigate those risks, and how risks will be reviewed during the project cycle. The implementer must have an internal due diligence process in place to monitor these risks. Proposals will not be approved without realistic risk assessment.

**4.** Projects should be budgeted in Pounds Sterling and demonstrate value for money. Budgets should give a detailed breakdown of cost per activity per month. For example, when budgeting for travel, details should be provided to show cost per person, per flight, including departure and destination cities class of travel and date window.

Strong proposals will spread the cost of the project throughout the year.

Proposals will not be approved without a detailed budget.

**5.** Payment will be made quarterly in arrears.

**6**. Projects must be completed by March 2015.

**Criteria for bid appraisal**

The Programme Board will consider projects against the following criteria:

1. Strategy, outcomes and impact:
	1. Response to National Cyber Security Strategy objectives.
	2. Relevance to a clearly defined and evidenced UK/ global priority security need, support for international values and an open internet, alignment with/ contribution to international development efforts, potential to improve co-ordination and effectiveness of existing Cyber Security Capacity Building efforts.
	3. Evidence of sustainability and scalability.
	4. Compatibility with the work of other cyber capacity building initiatives.
	5. Past performance of implementer.
2. Design
	1. Clarity
	2. Coherence and relevance of purpose, outputs, activities and indicators
3. Host government(s) and FCO Post support for the project and evidence of any wider stakeholder support and engagement.
4. Risk assessment adequacy, including around Human Rights, and evidence of an on-going due diligence mechanism.
5. Budget and value for money.
6. Monitoring and evaluation planning
7. Cross-cutting issue assessment including particularly human rights and value for money.

**Terms**

Agreements will be subject to FCO standard terms.

Proposals should be submitted to the Cyber Security Capacity Building Programme Team by **17:00** **Tuesday 27th MAY 2014.**

**Contacts:**

Programme Manager: Eleanor French

Deputy Programme Manager: Tracy Caulfield

1. Proposals focusing purely on research, analysis, seminars or workshops will not be relevant unless they clearly contribute to one of these aims. [↑](#footnote-ref-1)
2. In terms of both funding and recipient engagement: we strongly encourage projects that seek to secure future funding from other bodies for follow-on work or to become self-funding; bids must demonstrate the long term impact of the intended change. [↑](#footnote-ref-2)
3. Models that either already have a broad impact or are relatively efficient to apply more broadly. [↑](#footnote-ref-3)