Indonesia: call for proposals to enhance cyber security in the health sector

Objective

The objective of this project, under the Indonesia Digital Health Programme (Phase 1), is to start the implementation of two of these – to establish a Computer Emergency Response Team (CERT) and a multi-agency Health Data Protection and Cyber Security Coordination Group. Related UK funded work is supporting incident simulation training, a security outcomes framework and a privacy impact assessment of electronic medical record data. The implementer(s) of this project will be expected to maintain close alignment with these activities.

The Ministry of Health has recently created a Data Transformation Office, complementing the Centre for Data and Information. The digital platforms and services, however, are the responsibility of other delivery units. The incident response team will need to bring together resources from across the Ministry. The proposed Coordination Group will also include other ministries and agencies across the government.

The following guidance provides details of the requirements, the eligibility criteria and how to bid.

Timing and indicative budget

£200k from October 2021 to end March 2022

The establishment of health ministry Computer Emergency Response Team (CERT) and a multi-agency Health Data Protection and Cyber Security Coordination Group, will act as a focal point for strategic risk management relating to healthcare data and systems, an area which is currently lacking and undermines operational planning and incident response capability.

CERTs usually provide a combination of reactive services (e.g. alerts, warnings, incident response coordination) and proactive services (e.g. announcements, security assessments, development of tools). The MoH is already in discussions with BSSN over the remit and functions of their CERT, so an important area of this work will be selecting the right services to underpin the definition of the MoH CERT.

In terms of the Strategic Coordination Group, it is envisaged that the implementer will agree a terms of reference with key government stakeholders and support in setting up appropriate cross departmental governance structures focused on incident response strategies and threat intelligence sharing.

Please indicate in proposals:

- the foundational activities in the establishment of a CERT which will be delivered in the period
- the key agencies and organisations to be engaged in the Coordination Group and realistic (potential) agenda for the period
- proposed monitoring

Who can bid?

Bids are welcomed from not-for-profit organisations including academia, NGOs, inter-governmental organisations and not-for-profit arms of commercial entities.

Many capacity building projects cannot be fully delivered by a single implementer as the capability and skills required may only be found in a consortium. We therefore welcome bids from consortia, with a clear non-for-profit prime or lead implementer. Commercial organisations are permitted to join consortia as part of a bidding team. However, the commercial element of the proposal, which would be sub-contracted by the not-for-profit, must be proportionate.

Guidelines for submitting a proposal

See also:

Successful project proposal for funding will be announced by 22 September 2021. The British Embassy aims to sign grant agreements with the successful project implementer by 28 September 2021.

We will not consider proposals that are delivered after the submission deadline. All bid submissions must be in English. The Budget must be presented in pound sterling (GBP). Management and administrative costs shall not be more than 10% of the overall budget.

The impact of COVID-19 restrictions, including restrictions on local/international travel and in-person meetings/events should be factored in.

Bidders should not craft proposals in such a way to reach the budget ceiling. Bids should be constructed to specifically meet the objectives in pursuit of demonstrable impact and value for money. Bidders must submit a separate proposal and summarise it in the Project Proposal Form Part A. The Grant Agreement template is for review and information purpose only.

Criteria for assessing bids

Bids will be assessed against the following criteria:

- value for money – criteria for economy, efficiency, effectiveness, equity, and cost- effectiveness

- alignment with the requirements
- understanding of and familiarity with the local context
- project viability, including capacity and capability of implementing organisation(s)
- project design, including clear, achievable objectives/outputs/outcomes/impact
- good risk, issue and stakeholder management
- implementer experience, past performance
- sustainability

Background

As explained in the recently published Integrated Review, the UK's vision is to be a leading, responsible cyber power, working with partners to shape cyberspace according to our values. Our aim is to create a cyberspace that is free, open, peaceful and secure, and which benefits all countries and all people.

This programme will also align with HMGs country plan for Indonesia, particularly the KPIs around facilitating skills development in the health sector. It will directly contribute to delivering the KPI of improving Indonesia's National Cyber Security Plan which takes into account UK concerns and enhances protection of Indonesia's Critical national Infrastructure – of which health is one key sector. Indonesia is about to issue a National Cyber Security Strategy and Parliament is considering a Data Protection Law.

The health sector is vulnerable globally. In Indonesia, the threat to healthcare has been similarly singled out for attention; the Directorate of National Critical Information Infrastructure Protection within BSSN has produced an extensive Whitepaper on the state of cyber and information security in the Healthcare sector, stating that almost 69% of health institutions (based on their sampling) have weak cyber security levels and securing health data and systems is a key priority for the Ministry of Health . The development of digital health services is recognized as critical for increasing the quality of service and access to healthcare across this huge archipelago. Private systems have seen a huge increase in demand during the COVID restrictions but security concerns contribute to a lack of public trust in the services.

Previous work has made key recommendations for the development of cyber security capacity in the health system in Indonesia.