REQUEST FOR EXPRESSION OF INTEREST FOR SERVICES TO UPSCALE INFOSEC & PRIVACY PRACTICES

Country: **Republic of Korea**
Services: **Upscaling of organizational InfoSec & Privacy practices**
Closing Date: **18 September 2017**

Expression of Interest: EOI 2017/C/002

1.0 Introduction

The Green Climate Fund (the "GCF") was established in December 2010 with the purpose of making a significant and ambitious contribution to the global efforts towards attaining the goals set by the international community to combat climate change. In the context of sustainable development, the GCF will promote a paradigm shift towards low-emission and climate-resilient development pathways by providing support to developing countries to limit or reduce their greenhouse gas emissions and to adapt to the impacts of climate change.

The GCF was designated as an operating entity of the financial mechanism of the United Nations Framework Convention on Climate Change ("UNFCCC"). It is governed and supervised by a Board that has responsibility for funding decisions pursuant to the Governing Instrument for the Green Climate Fund. It is supported by an independent Secretariat, accountable to the Board, having management capabilities to execute day-to-day operations of the GCF, providing administrative, legal and financial expertise. The GCF's headquarters (the Secretariat) are located in Songdo, Incheon City, Republic of Korea.

The organization is life-cycle wise currently in its early rapid growth years. Business demands are evolving and increasing in a fast pace, so does the sophistication, scope and dependency on advanced interactive, collaborative information and knowledge management systems, tools and workflows.

GCF took advantage of its start-up situation for without legacy burdens architecting its solutions as being of Cloud first and only kind. In place and upcoming solutions are a careful combination of SaaS from strong mainstream vendors and - wherever differentiation is a strategic imperative - custom built systems relying on modern software frameworks.

By our very nature as international inter-governmental organization GCF is not directly bound by any national legislation. That said, we are as part of implementing our mandate daily dealing with confidential entrusted data from partners and contractors that must

be handled with outmost care. Respective bilateral contractual agreements are in place with a growing range of parties. At a state level, these include those defining immunities & privileges that are crucial for protecting GCF's workforce when performing their duties.

We have meanwhile in an evolutionary way reached a stage, where it becomes necessary for the organization to proactively further formalize, detail out and expand its information security and privacy programme.

2.0 Objectives and Scope of the Assignment

GCF follows an IT strategy of consciously preserving its agility and responsiveness by retaining and further expanding a major share of its IT activities through outsourcing arrangements. The current ratio of outsourcing is well above 50%. As far as information security and privacy concerns are affected this adds another layer of complexity, not necessarily risk, if well managed.

Via this Request for Expression of Interest we are looking for ideally one single subject matter expert, who is capable of competently covering both domains of expertise, information security as well as privacy (data protection).

Based on the expected feedback for this solicitation, and subsequent own discussions with our current two main IT outsourcing service providers (under renewable 3-year contract), we intend to use either a direct service contracting modality with the chosen one or two InfoSec/Privacy subject matter experts, or make use of the existing standing arrangements through our outsourcing service providers for doing so. Latter scenario might be more meaningful due to the already predictable triggering of additional non-trivial advisory and work demands in the domain of our current service providers, because of GCF's own upscaling initiative.

3.0 Modalities of Assignment

Approximately twelve months (October 2017 – September 2018), extendable, on an on-demand basis with monthly payments for agreed upon activities and against agreed upon daily rates that will differ between onsite and offsite work periods. We expect the clear majority of work to be of a remote and offline nature, requiring only infrequent real-time Skype interactions with GCF HQ personnel in South Korea and our contractor companies. GCF will compensate travel costs for periods needing physical presence in Incheon.

4.0 Request for Expression of Interest

The GCF now invites individual subject matter experts to indicate their interest in providing the services. Interested experts must provide detailed information indicating that they are qualified to perform the services (description of similar assignments, etc., see details of profile in Annex I). The Expressions of interest should contain comments on how the overall undertaking will be approached and expected inputs from GCF for execution of the assignment.

5.0 Qualifications of Expert(s)

Please refer to details in Annex I.

6.0 Selection of Expert(s)

The chosen service providing expert(s) will be selected in accordance with the procedures set out in GCF Administrative Procurement Guidelines. Information regarding these guidelines can be found at http://www.greenclimate.fund/documents/20182/574763/GCF_policy_-_Administrative_Guidelines_on_Procurement.pdf/b767d68e-f8b7-46d1-a18c-b6541f3dc010

Expression of Interest clearly marked "**Expression of Interest for services to upscale InfoSec and privacy practices**" can be submitted at the address below on or before **17:00 Korean Standard Time** on **18th September 2017:**

Green Climate Fund
175, Art Center-daero
Incheon 22004
Republic of Korea

Attention: Procurement Specialist

or through email using the following address: procurement@gcfund.org

Annex I

ToR, Data Protection/Privacy & Information Security Specialist

Nature of services expected:

- Drafting of policy documentation relating to privacy, data protection and information security, taking into consideration best practices and established data protection requirements.
- Mapping and documenting processes and data flows, identifying weaknesses and suggest improved controls and procedures.
- Contributing to the ongoing design, development, and maintenance of organizational privacy and data security programme and providing creative solutions to any concerns relating to data protection or cyber security that has been identified.
- Providing support to different functions within the GCF on matters related to privacy, data protection and information security, assisting the Fund to achieve its overarching transformative and long-term goals and objectives.
- Assessing cybersecurity risks for the organization, co-developing mitigation plans, and reporting on overall state of preparedness and fitness.
- Identifying, developing, implementing, and maintaining privacy and information security-related processes to ensure that corresponding assets and technologies are adequately protected.
- Organising and maintaining data protection and information security training programme for GCF staff, and ensuring that the training remains consistent with evolving privacy regulations, cybersecurity threats and organisational needs.
- Providing webinars, presentations and briefings to various organisational audiences.
- Additional operational tasks as assigned by the Director, Office of Risk Management & Compliance and the Head of ICT/CIO.

Expected experience and qualifications

- Advanced university degree, ideally in law, risk management, information security or information technology or related subjects.
- Good understanding and knowledge of regulations and best practices relating to privacy and data protection.
- 5+ years of experience in the practical application of national/international (for example EU General Data Protection Regulation) data protection/privacy regulations, as well as adherence to information security standards and best practises.
- Prior experience in developing or at least modernising organisational information security/privacy frameworks, programmes and authoring key underpinning internal regulations.
- Familiarity with important information security standards (ISO 27001) and applicable frameworks (COBIT).
- Sufficient technical breadth and depth in respect of a (mostly public and SaaS) Cloud centric, modern server-less custom build software based and mobile tech

based environment for competently and efficiently working with GCF's ICT team and its contractors.

- A professional information security related certification (Certified Information Security Professional - CISSP, Certified Information Systems Auditor - CISA or alike) is very desirable.
- Experience in planning, preparing and executing/accompanying an organisational certification project against a privacy and/or information security standard is very desirable.
- Experience from working in an international organization is an advantage.
- Work experience with international counterparts, and ability to work independently and take proactive initiative in response to the GCF's needs; and
- Fluency in English is essential (spoken and especially written); knowledge of another UN language an advantage.
