Clarifications

Request for Proposals "Hiring of Consultancy Services for Enterprise ISMS Gap Analysis" (No.T# 03 /18-19)

Clarifications issued in response to queries received before/during the pre-bid meeting held on **September 11, 2018** are as under:

Point	Queries	Clarifications/Response.
1.	We would like to request for 03 days extension in the date of submission of Proposals till Friday, 28th September 2018	Proposal/Bid opening shall take place as per schedule mention in the bidding documents, however, in case of any change in the schedule same shall be conveyed as per Rules.
2.	We understand that SECP reserves the right to cancel the RFP at any stage, however, making it a clause in Bid Submission Form against which Firm shall be signing does not seem to be a known practice. We request you to please remove point number (2) from the Bid Submission Form.	It is general clause and shall be applied if whole purchase process is to be withdrawn and will be informed as per Rules.
3.	Consultant hired for Enterprise ISMS Gap Analysis may recommend new/additional hardware/software. Whether the hired consultant be eligible to participate in the purchase process initiated for purchase of recommended hardware/software?	Hired consultant will not be eligible to participate in such purchase process. Ref: Procurement of Consultancy Services Regulations, 2010, Clause 4 i.e. Criteria for eligibility of consultants The procuring agency shall not hire a consultant for an assignment in which there is possibility of conflict of interest. If a consultant has been engaged by the procuring agency to provide goods or works for a project, it shall be disqualified from providing consulting services for the same project. Similarly, a consultant should not be hired for any assignment which by its nature, may be in conflict with another assignment of that consultant.
4.	Please clarify if we are required to review the technical security settings of Hosting Infrastructure, i.e. the Operating Systems and Databases? Please provide the details of the Operating Systems and Databases along with the version numbers, if we are required to review the same?	We have already prepared "**Information Assets Register(s)**' and based on these, we have identified critical assets in '**Asset Profile**'. This is prepared for conducting risk assessment. We do have Internal and External **Vulnerability Assessment and Penetration Testing Reports** conducted by 3rd party. Consultant doesn't have to perform vulnerability assessment or penetrating testing, again.

		Expected deliverable of these activities is '**Gap Analysis Report –on asset profiling, risk assessment and treatment methodologies**'. '
5.	Does SECP expect us to perform Internal and External Vulnerability Assessment and Penetration Testing as well OR just review the existing Reports? If Yes, then please provide the following information: • No. of Firewalls, Routers, Switches • No. of IP Addresses • No. of Servers No. of Applications	Consultant doesn't have to perform vulnerability assessment or penetrating testing, again.
6.	Does the project requires only ISMS training for SECP employees or ISO 27001 certification as well for selected employees? Also, please provide an estimated number for the employees that are expected to receive the training and awareness sessions.	After reviewing the adequacy of **information Security Awareness and Training (iSAT) Program Plan**, the selected consultant is will be assisting **iSAT Team** in conducting training and awareness sessions. Whereas, The '**Scope of the Work**" explains that the consultant shall conduct **Internal Audit Trainings for ISMS Audit Team**, and conduct or arrange trainings for CERT and BC&DR Teams.
7.	The expected duration to which SECP expects the project to last and when are they planning to go into the certification process (SECP tentative timelines)? Controls?	We are expecting that this consultancy project is to be **last for eight weeks**. After performing **at least one cycle of internal audit**, we may go for 3rd party certification audit against selected scope.
8.	What is the expected start date of engagement?	First week of October'2018
9.	Please specify the physical locations where the activity will be carried out i.e. number of offices, departments and locations. Does SECP plans to implement ISMS organization wide? Please also mention if any out station (other than ISB head office) visits will be required.	The physical location, where the activity will be carried out, is **SECP Head Office, NIC Building, Jinnah Avenue, Blue Area, Islamabad**. SECP plans to establish, implement, and continually improve enterprise ISMS, however, it may go for **certification against selected scope**.
10.	When was the information security policy developed and last reviewed? Is it approved from relevant authorities?	The **Enterprise Information Security Policy (EISP)** was approved in the Commission's 29th meeting of 2015 held on 23.06.2015. This EISP provides the **Information Security- Governance, Risk Management, and Compliance Council (IS-GRC Council)** the authority to oversee, direct, approve and coordinate the establishment of information security related policies. All

		HoDs are member of this council. This delegates the authority to the Chief Information Security Officer (CISO), as chairman of the council, to derive relevant policies, procedures etc. The IS-GRC Council is responsible for translating the Commission's directives into the information security policies and actions.
11.	Who are the possible stakeholders (internal and external) in this gap assessment engagement?	Possible stakeholders: **Internal** -SECP **External** -3rd party auditors
12.	Is there an initial assessment in place with regards to which ISMS Domains and Controls will be part of the scope?	We have documented scope, outlining the boundaries and applicability of the information security in **Enterprise ISMS Scope**. This document draws line on what is under the control of the ISMS and what is outside of it. This includes defining SECP's boundary and describing the operational environment, the security controls that are applicable to the system, and the system interconnections. Whereas, **Enterprise Information Security Policy (EISP)** provides an overview of the security requirements for the information processing systems.
13.	To what extent the IT-Services are outsourced by SECP?	Currently no IT application services are outsourced.
14.	When the Asset Register was last updated and reviewed? Moreover, we understand that consultancy firm will not be performing any management function, which includes assets profiling, to update assets register.	The '**Information Asset Register(s)**' were last updated and reviewed during December'2017. When consultant shall review our methodology on **Risk Assessment**, they may propose improve methodology. If new methodology is proposed, consultant may require documenting new '**Asset Profiling**" using currently available 'Information Asset Register(s)'.
15.	We understand that the consultancy firm will only review the Assets Management procedure(s) and methodologies followed by SECP, but will not be involved in updating or revising the assets register.	When consultant shall review our methodology on **Asset Management**, they may propose improve methodology. If new methodology is proposed, consultant may require populating new '**Information Asset Register(s)**'. However, we have nominated **ISMS-Point-of-Contacts (PoCs),** who can populate new asset registers, accordingly with minor training on new methodology.

16.	The scope of work requires us to 'Assist SECP teams' generally in each scope item. Can you please specify which particular activities do you think would form part of this action as 'assisting teams' is a very open ended statement.	The main driver of enterprise ISMS project is Information Security Department (ISD). This department uses Matrix Organization Structure, and borrows relevant resources from different departments, for performing particular ISMS activities. We have teams like: • ISMS-Point-of-Contacts (PoCs); • information Security Awareness and Training Team (iSATT); and • Information Risk Committee (IRC); Similarly, we have to build teams like: • information Security Incident Response Team (iSIRT); • InfoSec Aspects of Business Continuity & Disaster Recovery Team (InfoSec-BC&DR Team).
17.	The deliverables column of the RFP states "Any other relevant deliverables". Please clarify what SECP expects us to deliver other/additional deliverable documents that are not listed in this RFP? If Yes, please mention any additional deliverables.	When consultant thinks that "Scope of the Work" requires additional deliverables, they can mention them in their proposed response.
18.	The consultant after IMPLEMENTING all the ISMS processes (Assessment, documentation and validation) will require to provide ISO 27001 certification at the end?	The selected consultant cannot provide ISO 27001 certification services, as it will create a conflict of interest situation.
19.	After validation will the consultant provide the training or will just Assist SECP team in training?	The 'Scope of the Work" explains that the consultant shall conduct Internal Audit Trainings for ISMS Audit Team, and conduct or arrange trainings for CERT and BC&DR Teams.
20.	Will consultant need to allocate a dedicated member for monitoring and managed services after the ISMS implementation?	The 'Scope of the Work" does not require
21.	Referring to pre-bid meeting held at SECP Head Office, we would like to obtain further clarification with regards to the discussion of consultant firms role pertaining to Document Management System (DMS). We are not able to find any information related to DMS in the RFP document therefore, we are unsure of the scope of work that is expected to be performed under this domain. We shall be highly obliged if you could provide some information about this scope area while targeting specifically the objectives, key tasks and work products that are expected to be performed and deliver by the consultant firm.	DMS was discussed in the context of 'Scope of the Work' under clause 1.2. Wherein, it is stated 'Review current security practices, implementation adequacies with ISMS Documentation'. To implement 'Control of Document and Control of Record' clause of ISO 27001:2013 and SECP's related policy, we may require a DMS. The selected consultant's/firm's role would be 'recommending a suitable DMS, if

		required, for implementation adequacy'.
22.	Consultant hired for Enterprise ISMS Gap Analysis may recommend new/additional hardware/software. Whether the hired consultant be eligible to participate in the purchase process initiated for purchase of recommended hardware/software?	Hired consultant will not be eligible to participate in such purchase process. Ref: Procurement of Consultancy Services Regulations, 2010, Clause 4 i.e. Criteria for eligibility of consultants The procuring agency shall not hire a consultant for an assignment in which there is possibility of conflict of interest. If a consultant has been engaged by the procuring agency to provide goods or works for a project, it shall be disqualified from providing consulting services for the same project. Similarly, a consultant should not be hired for any assignment which by its nature, may be in conflict with another assignment of that consultant. Consultants can only give their recommendations specific products and also on upgrading of both software/hardware.
23.	Do consultant needs to propose new policies to fill the gaps discovered or just have to perform gap analysis?	Consultants have to perform gap analysis and if they find any gaps in documentation, they have to fill them.
24.	What is the intended Scope of this project (Departments, Processes, Section, Location, etc.)?	SECP, Head Office, NIC Building, Jinnah Avenue, blue area Islamabad.
25.	How many physical sites are to be included in the Certification? Please specify the location for each site.	We think only one site is required however consultant has to finalize certification sites.
26.	How many employees does your Scope have?	20 -50 employees for our proposed certification
27.	How many employees does your organization have?	500-1000
28.	Please indicate preferred start date and/or final deadline:	Start Date: First week of October 2018 End Date: Last week of November 2018
29.	How many business units (functional areas) do you have in your potential Scope?	More than two units.
30.	How many systems/servers/applications/devices in scope?	During last risk assessment, we have scoped six critical Information Systems.
31.	Does the organization have ISMS (Information Security Management System) in place?	Yes
32.	Does the organization follow a specific Risk Management Methodology?	Yes
33.	Does the organization use a specific tool to run Risk Management?	Yes, excel sheets with micros i.e. Risk Assessment Toolkit

<table>
<tr><td></td><td></td><td></td></tr>
<tr><td>34.</td><td>How often does your organization conduct risk assessments?</td><td>6-12 months.</td></tr>
<tr><td>34.</td><td>Does the organization have documented information security policies and procedure covering the following key areas (provide copy of the existed ones)?</td><td>
<table>
<tr><td>Security Policy</td><td>Yes</td></tr>
<tr><td>Acceptable Use Policy</td><td>Yes</td></tr>
<tr><td>Security Organization</td><td>Yes</td></tr>
<tr><td>Asset Classification</td><td>Yes</td></tr>
<tr><td>Access Controls</td><td>Yes</td></tr>
<tr><td>System Acquisition, Development & Maintenance</td><td>Yes</td></tr>
<tr><td>Physical Security</td><td>Yes</td></tr>
<tr><td>Business Continuity & DR</td><td>Yes</td></tr>
<tr><td>Human Resource Policy</td><td>Yes</td></tr>
<tr><td>Compliance</td><td>Consultant to identify ""Compliance Requirements</td></tr>
<tr><td>Communications Security</td><td>Yes</td></tr>
<tr><td>Incident Management</td><td>Yes</td></tr>
<tr><td>Operations Security</td><td>Yes</td></tr>
<tr><td>Cryptography Policy</td><td>We may not need it</td></tr>
<tr><td>Change Management</td><td>Yes</td></tr>
<tr><td>Document Control Procedure</td><td>Yes</td></tr>
<tr><td>Internal Audit Procedure</td><td>Yes</td></tr>
</table>
</td></tr>
<tr><td>35.</td><td>"Which trainings are part of the scope?</td><td>The trainings that are mentioned in bid document are mandatory and part of financials but consultant may suggest other trainings as well.</td></tr>
</table>