

# Leveraging ICT for Growth, Employment & Governance Project



## Bangladesh Computer Council (BCC)

Information and Communication Technology Division

Ministry of Posts, Telecommunications and Information Technology

ICT Tower, Plot # E-14/X, Agargaon, Dhaka-1207, Bangladesh

Phone: 8181392, 8181397 Fax: 8181383, E-mail: pd.lict@bcc.gov.bd

Memo No. 56.109.007.00.00.045.2017-3213

Date: May 03, 2017

### **Minutes of the Pre-bid meeting on Supply, Installation and Commissioning of Cyber Sensors into the Critical Information Infrastructure for Cyber Security (Contract Package# AF-G4):**

A Pre-bid meeting for the procurement of Goods for Supply, Installation and Commissioning of Cyber Sensors into the Critical Information Infrastructure for Cyber Security (Contract Package# AF-G4) was held on 29<sup>th</sup> March 2017 at 11:00 a.m. at the Conference Room of the Bangladesh Computer Council (BCC). The Pre-bid meeting was chaired by Mr. Rezaul Karim ndc, Project Director (Joint Secretary), Leveraging ICT for Growth, Employment and Governance Project. Project officials and representatives from potential bidders participated in the Conference (Attendance record is attached herewith as Attachment- 1).

2. The Chairperson welcomed the representatives of the potential bidders present in the meeting and explained the objectives of the project briefly. He then requested the participants to introduce themselves. After the introduction, the Chairperson requested to the Deputy Project Director of the project to make a presentation on the proceedings of the Bidding Document.
3. On invitation from the Chair the Deputy Project Director of the project delivered a power point presentation highlighting important milestones & guidelines to be followed in the procurement process. Deputy Project Director Mr. Tarique M. Barkatullah gave emphasis on important milestones. The last date of the bid submission is 26 April 2017 at 3.00 PM and the opening will be at 3.30 PM on the same date in presence of bidders' representatives (if present). He appraised the potential bidders to prepare their bids in compliance with the requirements specified in ITB, Bid Data Sheet, GCC & SCC clauses mentioned in the Bidding Document.
4. He informed the meeting that the selection method of the Goods is International Competitive Bidding (ICB). He clearly discussed the bid and bid security validity period. Bid validity will be 150 days after the deadline of bid submission and the bid security validity will be 28 days beyond the validity period of the bid i.e.178 days (150 plus 28 days).
5. After completion of the presentation session, the Chairperson opened the floor to for clarifications from the potential bidders' representatives present in the pre-proposal conference. Project Director requested the potential bidders to send their queries on or before 30<sup>st</sup> March 2017, 5.00 pm. He also informed that the authority has already received queries from two firms. The written response to the queries will be send in due time.

6. During discussion the project authority informed the meeting that the bid price will include three years warranty period.
7. The meeting was also informed that in the case of a Bidder who offers to supply and install major items of supply under the contract that the Bidder did not manufacture or otherwise produce, the Bidder shall provide the Manufacturer's Authorizations from the Manufacturer's Official Channel for the end user's territory (i.e. Bangladesh), using the form provided in Section IV, showing that the Bidder has been duly authorized by the manufacturer or producer of the related sub system or component to supply and install that item in the Purchaser's Country.
8. Project authority has received the following queries through email from the potential bidders. The responses are also provided against the queries (**Attachment-2**).
11. Having no other queries to be clarified, the meeting ended with a vote of thanks from the Chair.



(Md. Rezaul Karim, ndc)  
Project Director

Copy forwarded for kind information & necessary action with request to acknowledge receipt in writing within 2 days:

1. Mr. Maruf Al Mamun  
Sales Manager, JK Technosoft  
e-mail: [maruf.mamun@jktech.com](mailto:maruf.mamun@jktech.com)
2. Mr. Md. Ariful Islam  
Asstt. Manager, presales, Spectam Engineering Consortium Ltd  
7<sup>th</sup> Floor, Suite-C, 69/1, Panthapath, Chandrashila Suvastu Tower, Dhaka -1205.  
e-mail: [arif@spectrum-bd.com](mailto:arif@spectrum-bd.com)
3. Mr. Kazi Imdadul Islam  
JK Technosoft  
e-mail: [aunikislam12@gmail.com](mailto:aunikislam12@gmail.com)
4. Mr. Md. Wahid Uz Zaman  
CEO, Express Systems Limited  
House # 8/2, Riad # 01, Shamoly, Dhaka-1207.  
e-mail: [wahid.zaman@esl.com.bd](mailto:wahid.zaman@esl.com.bd)
5. Mr. Shahriar Bin Atique  
Head, Network Solution (Enterprise), Express Systems Limited  
House # 8/2, Riad # 01, Shamoly, Dhaka-1207.  
e-mail: [shahriar.atique@esl.com.bd](mailto:shahriar.atique@esl.com.bd)
6. Mr. Md. Somael Kabir  
Subject Matter Expert  
Technuf Limited, High Tower (9<sup>th</sup> floor), 9 Mohakhali C/A, Dhaka 1212.  
e-mail: [somael.kabir@technuf.com](mailto:somael.kabir@technuf.com)
7. Mr. Mahmudur Rahman  
Key Account Manager, Tech Valley Networks Limited  
Sharif Mansion (2<sup>nd</sup> Floor), 11 Mohakhali C/A, Dhaka 1212.  
e-mail: [mahmudur.rahman@tvnlbd.com](mailto:mahmudur.rahman@tvnlbd.com)
8. Mr. Maruf Ahmed  
OWIT  
e-mail: [maruf@oneworldinfortech.com](mailto:maruf@oneworldinfortech.com)
9. Mr. Sakil Md Tarikul Islam  
DGM & Head of ITES & Xaas  
Computer Services Limited  
House # 450, Road # 31, Mohakhali DOHS, Dhaka -1206.  
e-mail: [sakilislam@computerservicesltd.com](mailto:sakilislam@computerservicesltd.com)
10. Mr. Md. Hasan Imam  
Oculintech  
822/3 Begum Rokeya Sharani, Mirpur, Dhake -1212

- e-mail: [hasan@oculintech.com](mailto:hasan@oculintech.com)
11. Mr. Alamgir Hossain  
Shams & Sons  
e-mail: [alamgirhossain@gmail.com](mailto:alamgirhossain@gmail.com)
  12. Mr. Hasan Rahman  
Technology Director, DataSoft Systems Bangladesh Limited  
Rupayan Shelford (19<sup>th</sup> & 20<sup>th</sup> floor), 23/6 Mirpur Road, Shyamoli, Dhaka -1216.  
e-mail: [hasan.rahman@datasoft-bd.com](mailto:hasan.rahman@datasoft-bd.com)
  13. Mr. Ashiqul Islam Akhand  
Senior Project Manager & Enterprise Architect,  
DataSoft Systems Bangladesh Limited  
Rupayan Shelford (19<sup>th</sup> & 20<sup>th</sup> floor), 23/6 Mirpur Road, Shyamoli, Dhaka -1216  
e-mail: [mithu@datasoft-bd.com](mailto:mithu@datasoft-bd.com)
  14. Mr. Rumeer Choudhury  
COO  
Dactel Systems, House # CWN © 36, Road # 35, Gulshan-2, Dhaka-1212.  
e-mail: [rumeer@dactelsystems.com](mailto:rumeer@dactelsystems.com)
  15. Mr. Nirmal Kumar  
VP-Sales-South, East & SAARC  
Paladion Networks, 2<sup>nd</sup> floor, Shilpa Vidya, 49, 1<sup>st</sup> Main, JP Nagar 3<sup>rd</sup> Phase, Bangalore -  
560078, India.  
e-mail: [nirmal.kumar@paladion.net](mailto:nirmal.kumar@paladion.net)
  16. Mr. Mohasin Sohel  
CEO, ECL Systems Ltd.  
House 278 (2<sup>nd</sup> floor), Road 19, New DOHS, Mohakhali, Dhaka 1212.  
e-mail: [mohasin@msn.com](mailto:mohasin@msn.com)
  17. Mr. Tang Junwei  
Grentech  
e-mail: [masud@maishadsl-com](mailto:masud@maishadsl-com), [tangjunwei@powercn.com](mailto:tangjunwei@powercn.com)
  18. Mr. Abu  
ZTE  
e-mail: [a-bu@zte.com.cn](mailto:a-bu@zte.com.cn)
  19. Mr. Md. Murshid Sarker  
Sr. Engineer, Spectam Engineering Consortium Ltd  
7<sup>th</sup> Floor, Suite-C, 69/1, Panthapath, Chandrashila Suvastu Tower, Dhaka -1205.  
e-mail: [Murshid.sarker@spectrum-bd.com](mailto:Murshid.sarker@spectrum-bd.com)
  20. Mr. Md. Mafizur Rahman  
Wuhan Fiberhome International Technologies Co. Ltd.  
Bangladesh Branch Office: Unique Trade Center (UTC), Level-19, 8 Panthapath, Kawran  
Bazar, Dhaka -1215.



- e-mail: [mafizur@fiberhome.com](mailto:mafizur@fiberhome.com)
21. Mr. Tamzid Rahman Leo  
Cyber Security Specialist  
eGeneration Ltd, Saimon Center, 4<sup>th</sup> floor, House # 4/A, Road # 22, Gulshan -1, Dhaka.  
e-mail: [security@egeneration.com.bd](mailto:security@egeneration.com.bd)
  22. Mr. Md. Sayfuddin Shikder  
Asstt. Manager, Business Development  
eGeneration Ltd, Saimon Center, 4<sup>th</sup> floor, House # 4/A, Road # 22, Gulshan -1, Dhaka.  
e-mail: [sayfuddin.shikder@egeneration.com.bd](mailto:sayfuddin.shikder@egeneration.com.bd)
  23. Mr. Syed Jewel Kabir  
Relationship Manager  
SSL Wireless, 93 B New Eskaton Road, Dhaka -1212  
e-mail: [jewel.kabir@sslwireless.com](mailto:jewel.kabir@sslwireless.com)
  24. Mr. Bidhan Biswas  
Ernst & Young LLP, Gulshan Pink City, Suite 6/A, Level-7, Plot No. 15, Road No. 103,  
Block-CEN ©, Gulshan Avenue, Dhaka -1212.  
e-mail: [bidhan.biswas@bd.ey.com](mailto:bidhan.biswas@bd.ey.com)
  25. Mr. Md. Jalal Uddin  
Computer Services Ltd.  
e-mail: [jalal.t@computerservicesltd.com](mailto:jalal.t@computerservicesltd.com)
  26. Mr. Suman Kumar Saha  
AGM, System, Amber IT Limited, Navana Tower (7<sup>th</sup> floor), 45 Gulshan-1, Dhaka.  
e-mail: [suman@amberit.com.bd](mailto:suman@amberit.com.bd)
  27. Mr. A.K.M Shamsujjaman  
Edutech  
e-mail: [zaman@cybercloud.com.bd](mailto:zaman@cybercloud.com.bd)
  28. Mr. Tanmay Roy  
Wuhan Fiberhome Int. Tech. Co. Ltd.  
e-mail: [tanmay@fiberhome.com](mailto:tanmay@fiberhome.com)
  29. Mr. Arindam Ghosh  
JK Technosoft  
e-mail: [arindam.ghosh@jktech.com](mailto:arindam.ghosh@jktech.com)
  30. Mr. Dr. Vilius Benetis  
CEO, NRD CS, UAB  
Gyneju str. 16 LT-01109, Vilnius, Lithuania, EU.  
e-mail: [vb@nrd.no](mailto:vb@nrd.no)

(Md. Rezaul Karim, ndc)  
Project Director





## Leveraging ICT for Growth, Employment and Governance Project

## Bangladesh Computer Council (BCC)

Information and Communication Technology Division  
 Ministry of Posts, Telecommunications and Information Technology  
 ICT Tower, Plot # E-14/X, Agargaon, Dhaka-1207, Bangladesh.  
 Phone: 8181392, 8181397 Fax: 8181383, E-mail: plu.ict@bcc.net.bd

No.56.109.007.00.00.045.2017




Date: March 29, 2017


## Attendance of representatives of the Bidders

Pre-Bid Meeting for "Supply, Installation and Commissioning of Cyber Sensors into the Critic Information Infrastructure for Cyber Security (Contract Package # G4)"

Time: 11:00a






SL	Name and Designation	Name of the Firm	Contract Cell no and e-mail	Signature
1.	Masruf Al Mamun Sales, Manager	JK Technosoft	01997722781 masruf.mamun@ jkttech.com	
2.	Md. Anisul Islam Asst. Manager	Spectrum Engg.	01716258466 anil@ spectrum- bd.com	
3.	Kazi Imdadul Islam	JK Technosoft	01683301728 aunikislam12 @gmail.com	
4.	Md. Wahid Uz Zaman CEO	ESL	01755513839 Wahid.zaman @esl.com.bd	

SL	Name and Designation	Name of the Firm	Contract Cell no and e-mail	Signature
5.	SHAHRIAR BIN ATIQUE	ESL	01973146143 shahriar.atique @esi.com.bd	
6.	MD. SOMAEL KABIR	TECHNUS	01755557296 <del>SOMAEL. KABIR</del> <del>@TECHNUS</del> COM SOMAEL.KABIR@TECHNUS.COM	
7.	Mahmudur Rahman	Tech Valley Networks Ltd.	01847082976 mahmudur.rahman @tvnlbd.com	
8.	Maruf Ahmed	OWIT	01713452680 marufe@ oneworldinfotech com.	
9.	SAKIL ISLAM	Computer Services Ltd.	01616160366 SAKILISLAM@ COMPUTERSERVICES LTD.COM	

SL	Name and Designation	Name of the Firm	Contract Cell no and e-mail	Signature
10.	Md. Hasan Faram	Oculin tech BD Ltd.	01871001797 # Hasan@oculinteel.com	
11.	ALAMGAR HOSSAIN	SHAMS & SONS	0172606405 ALAMGARHOSSAIN@GMAIL.COM	
12.	HASAN RAHMAN	DataSoft	01937999532 hasan.rahman@datasoft-bd.com	
13.	ASHIQUUL ISLAM AKHAND	DataSoft	01818012932 mithe@datasoft-bd.com	
14.	RUMEE GHOSHARY COO	DACTEL SYSTEMS	01733538281 RUMEE@DACTELSYSTEMS.COM	

nb



SL	Name and Designation	Name of the Firm	Contract Cell no and e-mail	Signature
15.	NIRMAL KUMAR VP. SALES	PALADION NETWORKS	+91 88612 30811 +91 98453 19101 nirmal.kumar @ Paladion, net	
16.	Md. Mokasim Sohel	ECL Systems	01841-456910 mokasim@msu.com	
17.	Tang Junwei	Grentech	masud@maishadsl.com + tangjunwei@ powerch.com	
18.	Abu <del>Hikang</del>	ZTE	a.bu@zte.com.cn 01754-8855 77	Abu <del>Hikang</del> 
19.	MURSHID SARKER	Spectrum Engineering consortium Ltd	01722390678	



20. M Faysal Zaman level 3 +8801733503193 ~~z~~ Kaysal@gmail.com  
Caricover.com
21. Md. Mafizur Rahman Wuhon Fiberhome Int. Co. Ltd. 01760029636 mafizur@fiberhome.com
22. Tamzid Rahman eGeneration Ltd. 01737923848  
tamzid.lee@e-generation.com.bd
23. Saifuddin Shikder eGeneration Ltd. 01823328673  
info@e-generation.com.bd
24. Jewel Hossain SSL jewel.hossain@ssl.com.bd
25. Bidhan Biswas EY bidhan.biswas@bd.ey.com
26. Md. Jalal Uddin CSL JALAL.T@COMPUTERSERVICESLTD.COM
27. Sumon Kumar Saha Amber IT suman@amberit.com.bd
28. A.K.M Shamuzzaman EduTech zaman@cybercloud.com.bd
29. Tanmay Roy Wuhon Fiberhome Int. Tech. Co. Ltd. tanmay@fiberhome.com
30. Arindam Ghosh JK Technosoft arindam.ghosh@jktech.com
31. dr. Vilas Beretis NRDA VB@NRD.NO

do

**Responses of Queries for Supply, Installation and Commissioning of Cyber Sensors into the Critical Information Infrastructure for Cyber Security (Contract Package# AF-G4)**

This is for information of all concerned bidders that Instructions to Bidders (ITB) and General Conditions of Contract (GCC) clauses cannot be modified in any manner. Where an ITB or GCC clause contains reference to the Bidding Data Sheet (BDS) or Special Conditions of Contract (SCC) respectively, additional or specific information is written into the corresponding BDS or SCC clause to amplify or clarify the main BDS or SCC clause. Some of the BDS or SCC clauses may be subsequently modified as a result of suggestions received from bidders. However the BDS and SCC can never be used to circumvent in any way the intent of the parent ITB or GCC clause.



Subject: Response to Pre-bid Queries (Technical)						
Serial #	Section	Page #	Existing Specification / Condition /Clause	Bidder's Change/ Add/ Delete request	Bidder's Remark	Purchaser's Remark
1	VII	P125	1.5.1.2 The proposed cyber sensors must meet the following performance indicators: Analyze and Indicate Surface Area Risks – known devices reporting. Blind spots and unknown systems increase risk.	What does the "Surface Area Risks" mean?	<p>1.5.1.2 The proposed cyber sensors must meet the following performance indicators:</p> <ul style="list-style-type: none"> <li>• Discover New Threats – events not seen before. New types of threats are less likely to be covered by an existing prescription, increasing risk.</li> <li>• Ensure Defense Effectiveness – recurring defense activity. Recurring threats signify ineffective defenses, increasing risk.</li> <li>• Find Opportunity Risk – severity of events. More serious threats and vulnerabilities are more likely to lead to compromise.</li> <li>• Measure Technical Debt – volume/velocity/acceleration/severity of events. The combination increases team backlog and risk.</li> <li>• Provide Secure History – confidence measure. Understanding risk requires sufficient data.</li> <li>• Analyze and Indicate Surface Area Risks–known devices reporting. Blind spots and unknown systems increase risk.</li> <li>• State of Health of Sensors – Availability of sensor operations and security resilience from external threats.</li> </ul>	<p>Surface Area Risks are the risks concerning different points (the "attack vectors"), where an unauthorized user (the "attacker") can try to enter data to or extract data from an environment. The environment could be any information system and/or any network system. <b>Example Scenario:</b> When an e-commerce site is in the external zone, you increase the risk of attack to your e-commerce application resources. The risk increases with every feature you provide or service you expose because you increase the size or surface area of your exposed application. Surface area is a key security consideration in the development and configuration of your e-commerce site. As each enterprise has countless potential vulnerable points, there has been increasing advantage for hackers and attackers as they only need to find one vulnerable point to succeed in their attack. According to the white paper of Skybox Security (<a href="https://www.skyboxsecurity.com/sites/default/files/Attack%20Surface%20Visualization.pdf">https://www.skyboxsecurity.com/sites/default/files/Attack%20Surface%20Visualization.pdf</a>), there are three steps towards understanding and visualizing an attack surface: Step 1: Visualize. Visualize the system of an enterprise is the first step, by mapping out all the devices, paths and networks. Step 2: Find Indicators of Exposures. The second step is to correspond each indicator of a vulnerability being potentially exposed to the visualized map in the last step. Step 3: Find Indicators of Compromise. This is an indicator that an attack has already succeeded.</p>

Subject:		Response to Pre-bid Queries (Technical)																	
Serial #	Section	Page #	Existing Specification / Condition / Clause	Bidder's Change/ Add/ Delete request	Bidder's Remark	Purchaser's Remark													
2	VII	P130	3.1.3 Detailed Technical Requirements, Item-1: Detailed design for the implementation and customization of Cyber Sensors, SL.#.1 General, Detail design of the implementation and customization of lab should be provide.	Mentioned need the lab, but no detail introduction of this part. Could you provide more specific requirements about the lab? And please provide the detail design of the implementation and customization of the lab.	<p>3.1.3 Detailed Technical Requirements</p> <table border="1"> <thead> <tr> <th colspan="3">Item-1: Detailed design for the implementation and customization of Cyber Sensors</th> </tr> <tr> <th>SL. #</th> <th>Product Name/Items</th> <th>Description of requirements</th> <th>UoM</th> <th>QTY</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>General</td> <td> <p>Detail design of the implementation and customization of lab should be provided covering:</p> <ol style="list-style-type: none"> <li>1. Detail technical and functional architecture of the deployable Cyber Sensors, and interconnection with Cyber Sensors Management Module.</li> <li>2. Services model and description.</li> <li>3. Sensors Operational program.</li> <li>4. Implementation project plan.</li> <li>5. Resources required to establish and run the Sensors.</li> </ol> <p>Document should include designs for all items of the contract.</p> </td> <td></td> <td></td> </tr> </tbody> </table>	Item-1: Detailed design for the implementation and customization of Cyber Sensors			SL. #	Product Name/Items	Description of requirements	UoM	QTY	1	General	<p>Detail design of the implementation and customization of lab should be provided covering:</p> <ol style="list-style-type: none"> <li>1. Detail technical and functional architecture of the deployable Cyber Sensors, and interconnection with Cyber Sensors Management Module.</li> <li>2. Services model and description.</li> <li>3. Sensors Operational program.</li> <li>4. Implementation project plan.</li> <li>5. Resources required to establish and run the Sensors.</li> </ol> <p>Document should include designs for all items of the contract.</p>			The ultimate goal of the assignment is to build a laboratory-based sensor network, which will be permanent and support practically any application, and capable of taking full advantage of the potential of cyber sensing technology. The specific requirement is to set up a cyber sensor lab with a sensing network that would include passive sensor (TAP), active sensor (honeypot type) and active sensor (radar type).
Item-1: Detailed design for the implementation and customization of Cyber Sensors																			
SL. #	Product Name/Items	Description of requirements	UoM	QTY															
1	General	<p>Detail design of the implementation and customization of lab should be provided covering:</p> <ol style="list-style-type: none"> <li>1. Detail technical and functional architecture of the deployable Cyber Sensors, and interconnection with Cyber Sensors Management Module.</li> <li>2. Services model and description.</li> <li>3. Sensors Operational program.</li> <li>4. Implementation project plan.</li> <li>5. Resources required to establish and run the Sensors.</li> </ol> <p>Document should include designs for all items of the contract.</p>																	

Subject: Response to Pre-bid Queries (Technical)						
Serial #	Section	Page #	Existing Specification / Condition /Clause	Bidder's Change/ Add/ Delete request	Bidder's Remark	Purchaser's Remark
3	5. Eligible goods and services: 5.2	P12	For the purposes of this bidding document, the term "Information System" means all:	For the purpose of this bidding document, as the term "information system" is defined, we also request for defining terms "cyber sensor(s)" and "Critical Information Infrastructure (CII)".	<p><b>F. SERVICE SPECIFICATIONS--RECURRENT COST ITEMS</b></p> <p>5.F.1 Warranty Defect Repair</p> <p>5.F.1.1 The Supplier MUST provide the following services under the Contract as a separate order separate contracts (as specified in the bidding documents)</p> <p>5.F.1.1.1 Warranty Defect Repair Services: Three (3) years warranty should provide to all equipments, systems, and hardware and software items. Furthermore three (3) years software licenses of each will every reinstallation must be facinated along with three years hot support including labor, spare parts, updates and/or upgrades.</p> <p>5.F.1.1.2 Technical Assistance: Supplier should provide Technical assistance on call base during warranty period. Response time must be less than 2 hours and resolution time must be less than 6 hours.</p> <p><u>Important Note:</u> All costs of the above mentioned services must be included in the unit cost in the bidding price. There will be no reserve cost come in this tender.</p>	<p>A cybersecurity sensor collects data and sends it to the analytic grid for processing. The role of the sensor in our conceptual model is to detect things. To get to the next step, requirements, we need to determine:</p> <ul style="list-style-type: none"> <li>• Where to detect</li> <li>• What to detect</li> <li>• How to detect</li> <li>• How to forward</li> <li>• How to analyze</li> <li>• What to analyze</li> <li>• What not to analyze</li> <li>• What do we want after analyzing</li> </ul> <p>We believe that the potential bidders understand our requirement from what has been mentioned in the request for bids and are capable of proposing architecture and solution for BCC. We do not want to shed more light on this.</p> <p>The Critical Information Infrastructure (CII) refers to the information facilities concerning the national security, the national economy and the people's livelihood of Bangladesh, which may seriously damage the national security and the public interest if the data is divulged, destroyed or lost, including but not limited to providing public communications, broadcasting and television transmission and other services. Information network, energy, finance, transportation, education, scientific research, water conservancy, industrial manufacturing, medical and health, social security, public utilities and other important information systems and important Internet applications.</p>

<b>Subject: Response to Pre-bid Queries (Technical)</b>						
<b>Serial #</b>	<b>Section</b>	<b>Page #</b>	<b>Existing Specification / Condition /Clause</b>	<b>Bidder's Change/ Add/ Delete request</b>	<b>Bidder's Remark</b>	<b>Purchaser's Remark</b>
4	1.2.1.2	P121	Government of Bangladesh requires strategic cyber oversight of Critical Information Infrastructures (CII) by developing, deploying and maintaining coordinated cyber visibility across CII organizations.	We request you to provide information on CII organizations in a document to study and understand the stance of security needed for each of those, expecting those critical sectors are already identified. Also their location in the country so that project execution planning and dependencies could be identified.	None	The requested information would only be provided to the finally selected bidder on signing a non-disclosure agreement after issuance of notification of award
5	1.2.1.3	P121	Aggregation and analysis of information through Cyber Sensors, Government of Bangladesh make informative decisions	We request you to provide more clarity on the process/analysis of information which is disseminated by cyber sensors as this requirement is more equivalent to the agents deployed in an SIEM environment.	None	Potential bidders are expected to understand this requirement. No more clarification would be provided.

Subject:		Response to Pre-bid Queries (Technical)				
Serial #	Section	Page #	Existing Specification / Condition /Clause	Bidder's Change/ Add/ Delete request	Bidder's Remark	Purchaser's Remark
6	1.3.1.1	P122	<p>The Information System MUST be supplied and configured to implement the following architecture. Software Architecture consists of the following modules:</p> <p>1. Management Module 2. Network Module; Management Module consists of the following logical components:</p> <p>1. Intelligence database with dashboard and reporting software; 2. Configuration software; 3. Sensors monitoring software. Network Module consists of the following software components:</p> <p>1. Sensing software 2. TAP (Network Tap) technology software; 3. VPN termination technology software.</p>	<p>Please clarify on:</p> <p>1. What is intelligence database (Is that same as threat intelligence database or the data collected from the sensors?) 2. Sensors monitoring software 3. Sensing software (is that identical to multiple collection of agents). Also, we request BCC to kindly elaborate in details the requirement for better understanding.</p>	None	Potential bidders are expected to understand this requirement. No more clarification would be provided.



<b>Subject:</b> Response to Pre-bid Queries (Technical)						
<b>Serial #</b>	<b>Section</b>	<b>Page #</b>	<b>Existing Specification / Condition /Clause</b>	<b>Bidder's Change/ Add/ Delete request</b>	<b>Bidder's Remark</b>	<b>Purchaser's Remark</b>
7	1.5.1.2	P125	The decisive performance level that BCC wants to have from the proposed Cyber sensors is to have the highest level of confidence in the overall health of IT security operations that ultimately aid decision makers in assigning priorities within a business context.	We request for providing us more clarity on technicalities of overall health of IT security operations. This explains there is a need of bringing managed security operations i.e., more of a Security operations centre (SOC) into picture.	None	BCC does not require Security Operations Center (SOC) under this bid.
8	2.1.1.1	P126	An in-depth study of cyber security threats and requirement needs for sensing the threats and to have complete visibility of cyber infrastructure to identify indicators of compromise is required to be performed by the selected vendor. In the end of the detailed analysis stage the selected vendor must submit a detailed analysis report.	Please confirm the levels of analysis and the number and type of systems (only IT as well as ICS) to be analyzed under detailed incidence response and forensic analysis. Kindly elaborate.	None	The expected level of analysis is the lowest level that is the most detailed technical level of incidence response and forensic analysis including finding of indicators of exposure. Regarding type of systems BCC wants to confirm that both IT and ICS (SCADA) systems are under consideration.

Subject:		Response to Pre-bid Queries (Technical)				
Serial #	Section	Page #	Existing Specification / Condition /Clause	Bidder's Change/ Add/ Delete request	Bidder's Remark	Purchaser's Remark
9	2.3.1.1	P126	The selected vendor must provide integration services for the Cyber Sensors to receive and analyze data from SIEM system, Firewall, IPS, Routers, Switches, Flow Analyzer, Anti APT system, Email Security Gateway, Network Monitoring System, etc.	Please clarify on other security infrastructure if already installed. Is this system integration mentioned is about CIRT architecture? We assume Cyber sensors and SIEM are contradictory technologies typically performs same operations in any environment. Does cyber sensors also represent agents/collectors in an SIEM system Request you to kindly elaborate in details for better understanding.	None	Answer of Q1: The security architecture is conventional with IPS, Firewall, Anti APT, SIEM, email security gateway, network monitoring system. This security infrastructure is already installed. The system integration is mentioned is with CIRT. Answer of Q2. A Log manager with a built-in rules and a correlation engine is known as a SIEM system. The SIEM system is designed to analyze logs from various different sources and generates an alert if certain conditions are met. Whereas BCC is looking to deploy Cyber Sensors, which are applications or appliances that capture user and application data by analyzing network traffic as it flows around a network. This information which is sometimes referred to as metadata, is then stored in a database so that it can be used for real time or historical analysis of security or operational problems. BCC wants to deploy passive sensors (TAP), active sensors (honeypot type) and active sensors (radar type).
10	3.1.3 Item-2	P130	CSMM license must support collecting of at least 5000 events per second for deployable 15 critical information infrastructure sites	We would request you to clarify whether the events per second mentioned is for each site or all sites. This clause is not clear. Request you to kindly elaborate in details for better understanding.	None	The events per second mentioned is for each site, aggregated into total amount at the platform.
11	Section VII - 1.3.1.2	P122	VPN termination technology software	Clarification Needed	This is needed as part of the network module. Is this technology being requested to connect the Network Module (CSNM) with CSMM? With respect to the VPN technology, are there any such software products that BCC is already using to set up VPNs? Or do we need to quote for the VPN solution?	Answer to Q1: Yes Answer to Q2: Resilient and strongly secured VPN solution should be provided, independent from what BCC uses now, which would be used only for interconnecting sensors.

<b>Subject:</b> Response to Pre-bid Queries (Technical)						
<b>Serial #</b>	<b>Section</b>	<b>Page #</b>	<b>Existing Specification / Condition /Clause</b>	<b>Bidder's Change/ Add/ Delete request</b>	<b>Bidder's Remark</b>	<b>Purchaser's Remark</b>
12	Section VII - 1.3.1.2	P122	VPN termination technology software	Confirmation needed	The leased line connectivity between CSNM and CSMM over which the VPN will operate will be provided by BCC. Kindly confirm.	There are no leased lines in the solution, VPNs are carried out over existing networks.
13	Section VII - 1.3	P122	Transaction volumes at CSMM	Information required	What are the anticipated transaction volumes (in Transactions Per Second) at the Cyber Sensors Management Module (CSMM)? This volume information will enable us to design the CSMM module for adequate capacity.	It should accommodate sensor traffic from moderate to big size of Bangladesh organizations, as sensors will be placed at organizations in critical infrastructure sectors of Bangladesh. It should sustain the expected traffic growth through the next several years in these organizations.
14	Section VII - 1.3	P122	Transaction volumes at the Network Module (CSNM)	Information required	What is the anticipated transaction volumes (in Transactions per Second) at each of the 15 Network Modules? This volume information will enable us to design the Network module for adequate capacity.	It should accommodate sensor traffic from moderate to big size of Bangladeshi organizations, as sensors will be placed at organizations in critical infrastructure sectors of Bangladesh. It should sustain the expected traffic growth through the next several years in these organizations.
15	Section VII - 1.3	P122	Location of the Network Module (CSNM)	Information required	It is mentioned in the RFP that there are 15 Network Modules. Can the location of each of the Network Module be provided? This will enable us to plan for deployment adequately based on the geographical spread.	Up to 70% of sensors is expected to be placed in Dhaka region, remaining might be placed at the main data hubs in Bangladesh
16	Section VII	P121	Testing environment	Information required	Will BCC be able to provide a environment for UAT before moving the systems into production. Should hardware budget include the hardware needed to setting up a UAT environment for testing the deliveries by BCC before releasing into production?	Bidder is responsible to provide all hardware and software needed for the project.
17	Section VII – 1.4.1.6	P125	Disaster Recovery	Information required	Is the expectation to provide disaster recovery centre for each of the 15 Network modules and the central CSMM? Please provide an outline of the scope of the disaster recovery that is required?	BCC wants to build a setup for disaster recovery platform, which will consist of hardware, software and storage for backing up data in a centralized location, which will be connected with 15 critical information infrastructures. BCC does not need synchronous real time data replication. But data must be backed up periodically after every 30 minutes interval. VPN connections would be used for data backup. The bidder must provide all documentation regarding disaster recovery procedure. And the Bidder needs to cover the scenario of components, nodes, and systems.

<b>Subject: Response to Pre-bid Queries (Technical)</b>						
<b>Serial #</b>	<b>Section</b>	<b>Page #</b>	<b>Existing Specification / Condition /Clause</b>	<b>Bidder's Change/ Add/ Delete request</b>	<b>Bidder's Remark</b>	<b>Purchaser's Remark</b>
18	Section VII – 2.3.1.1	P126	List of Network devices	Information required	Please provide details on the type and version of each of these products that would need to be interfaced?	Routers: Cisco and Huawei, Switches: Cisco and Huawei, SIEM- Log Rhythm, NMS - Everest, Nagios, Application Monitoring - Zabbix, WAF-Penta, B/W Manager - Procera, Forensics - Balabit, Netflow - Lancope, AAA - Cisco, Anti APT - Stealthwatch, email security - Ironport
19	Section VII – 2.3.1.1	P126	List of Network devices	Information required	SIEM – what are the SIEMs used by BCC that need to be supported?	Answer is included above in point 18
20	Section VII – 2.3.1.1	P126	List of Network devices	Information required	Firewall – what firewalls need to be supported and interfaced?	Answer is included above in point 18
21	Section VII – 2.3.1.1	P126	List of Network devices	Information required	IPS – what IPS systems will need to be supported and interfaced?	Answer is included above in point 18
22	Section VII – 2.3.1.1	P126	List of Network devices	Information required	Routers – what router types will need to be supported?	Answer is included above in point 18
23	Section VII – 2.3.1.1	P126	List of Network devices	Information required	Switches – what types need to be supported?	Answer is included above in point 18
24	Section VII – 2.3.1.1	P126	List of Network devices	Information required	Flow Analyzers – What types need to be supported?	Answer is included above in point 18
25	Section VII – 2.3.1.1	P126	List of Network devices	Information required	Anti APT Systems – what types are being used by BCC?	Answer is included above in point 18
26	Section VII – 2.3.1.1	P126	List of Network devices	Information required	Email Security Gateways – what email gateways are being used by BCC?	Answer is included above in point 18
27	Section VII – 2.3.1.1	P126	List of Network devices	Information required	Network Monitoring Systems – what systems are being used by BCC?	Answer is included above in point 18
28	Section VII – 2.7.1	P126	Requirements of the Supplier's Technical Team	Information required	Are these people to be made available at the location of CSMM centre?	Yes. These people must be available at the location of CSMM Centre.

Subject:		Response to Pre-bid Queries (Technical)				
Serial #	Section	Page #	Existing Specification / Condition /Clause	Bidder's Change/ Add/ Delete request	Bidder's Remark	Purchaser's Remark
29	Section VII – 3.1.2 – 1	P129	Operations must be supported for 36 months of maintenance services after system commissioning	Information required	Does this mean the people listed in 2.7.1 should be available onsite at Bangladesh for 36 months?	During the deployment at each site there should be people on site. All of the human resources do not need to be available for 36 months. Human Resources must be planned very carefully to ensure that right person is available at the right time, however the project might need more similar competent people to deliver project on time.
30	Section VII – 3.1.3 Item 2	P130	Integration with CIRT processes	Information required	What is the incident handling system that CIRT is using? Are API specs available for integration?	CIRT is using common CSIRT incident handling systems. RESTfull APIs and other integrations are supported.
31	Section VII – 3.1.3 Item 3	P132	Deep Packet Inspection	Information required	Our assumption is that it pertains to capturing of all non-encrypted traffic. Please confirm.	It must capture all data.
32	General		Data retention	Information required	What is the data retention period that is required?	. At least one week for raw data and at least three months for analyzed data.
33	Section 2.4.2 Specific Experience	P58	Participation as a prime supplier, management contractor, JV1 member, sub-contractor, in at least one (01) contracts within the last five (05) years, each with a value of at least US\$ 1 million or equivalent amount, that have been successfully and substantially completed and that are similar to the proposed Information System.	Clarification required	Can the scope of work of such a contract be in the area of "Security Operations Monitoring"? Will such an order/contract be considered as similar or representing the nature of this RFP?	yes

<b>Subject:</b>		<b>Response to Pre-bid Queries (Technical)</b>				
<b>Serial #</b>	<b>Section</b>	<b>Page #</b>	<b>Existing Specification / Condition /Clause</b>	<b>Bidder's Change/ Add/ Delete request</b>	<b>Bidder's Remark</b>	<b>Purchaser's Remark</b>
34	General		High Availability	Add	The RFP does not specify requirements towards high availability. Is this required and if required, can specifications for the requirement be provided?	High availability for central servers and VPN terminations points must be considered
35	2.1.1.1	P126	An in-depth study of cyber security threats and requirement needs for sensing the threats and to have complete visibility of cyber infrastructure to identify indicators of compromise is required to be performed by the selected vendor. In the end of the detailed analysis stage the selected vendor must submit a detailed analysis report. This report, if agreed by the purchaser will be the basis of functional requirements and in the light of this report the design of the proposed cyber sensors platform will be made.	Information required	Has the study of cybersecurity threats and requirement needs for sensing the threats (noted in section 2.1.1.1) been completed? (a) Can we have a copy of the report? (b) Without the results of this study, vendor will not know which IoCs will be monitored or what business or functional requirements are in the scope of this project.	Answer 1: A study of cybersecurity threats and requirements has been performed by the BGD e-Gov CIRT. Answer 2: For scoping out the solution this report is not necessary, because BCC expects all Indicators of exposure and all indicators of compromise to be monitored. However after signing of a NDA the report could be shared with the vendor with whom BCC will come into an agreement for this project. The document is a highly classified and cannot be shared at this time.

<b>Subject:</b>		<b>Response to Pre-bid Queries (Technical)</b>				
<b>Serial #</b>	<b>Section</b>	<b>Page #</b>	<b>Existing Specification / Condition /Clause</b>	<b>Bidder's Change/ Add/ Delete request</b>	<b>Bidder's Remark</b>	<b>Purchaser's Remark</b>
36	2.3.1.1	P126	The selected vendor must provide integration services for the Cyber Sensors to receive and analyze data from SIEM system, Firewall, IPS, Routers, Switches, Flow Analyzer, Anti APT system, Email Security Gateway, Network Monitoring System, etc.	Information required	Cyber Sensors should be able to receive and analyze data from SIEM system, Firewall, IPS, Routers, Switches, Flow Analyzer, Anti APT system, Email Security Gateway, Network Monitoring System, etc. (a) Are these network components in place? Can we have names of vendors / brands for each component to ensure that our solution is integrated with the desired tools and technologies?	Answer is included above in point 18
37	1.4.1.3	P124	This is a turnkey assignment. The winning bidder will be responsible for operational monitoring, diagnostics and troubleshooting of the installed systems/equipments . Under the scope the selected bidder shall undertake monitoring, administration, management and maintenance of the entire cyber sensor infrastructure supplied, installed and commissioned by them under this tender.	Clarification required	3-year maintenance requirement is clarified elsewhere in the document but what are the expectations around monitoring, administration, and management of the honeypot? Does the scope include separate hardware installation for honeypot or is the expectation to install honeypot on existing or covered hardware?	Three (3) years warranty including maintenance of honeypot is required. The scope includes complete solution for active sensing via honeypot (could be appliance based or software based that is installed in a computer), in either case the entire solution must be provided by the bidder. Regarding monitoring, administration and management of the honeypot, BCC wants the supplier to provide 3 years warranty including support and maintenance services on call basis. And full replacement (if needed) during the warranty period.

Subject: Response to Pre-bid Queries (Technical)						
Serial #	Section	Page #	Existing Specification / Condition /Clause	Bidder's Change/ Add/ Delete request	Bidder's Remark	Purchaser's Remark
38	3.1.3 Item # 3	P132	Cyber Sensors Network Module (CSNM)	Clarification required	1. Does the scope include separate hardware installation for honeypot or is the expectation to install honeypot on existing or covered hardware? 2. As Per 3.1.3 item 3, CSNM must be provided as a transportable rack-on-wheels solution, deployable for each CII organization. Will honeypot be installed on the same rack or different racks? Can we use Containers? 3. Will the honeypot be installed within the same geography/network or different geographies? 4. What are the measures of success or key metrics?	Answer to Q1: The scope includes complete solution for active sensing via honeypot (could be appliance based or software based that is installed in a computer). Answer to Q2: Yes. honeypot would be installed in the same rack. Containers can be used. Answer: Most of them would be installed in Dhaka (70%) and a few (30%) in other districts of Bangladesh. Answer to Q4: Honeypot should be provided in the solution, and be part of sensor solution as described in ToR. Basic required metrics are defined, Bidder is expected to articulate additional relevant metrics relevant to the proposed solution.
39	2.3.1.1	P126	The selected vendor must provide integration services for the Cyber Sensors to receive and analyze data from SIEM system, Firewall, IPS, Routers, Switches, Flow Analyzer, Anti APT system, Email Security Gateway, Network Monitoring System, etc.	Clarification required	Q1. Any concerns with running solution on Virtual Machines instead of dedicated hardware for each instance? Thought is to use combination of dedicated machines and VM for better performance and optimization? Q2. Can you share the names of the SIEM system & some of the other data sources mentioned in 2.3.1.1 ? For those that we may not integrate with today, would it be possible to get sample logs sometime in future so we can write parsers? Q3. Is it possible to get Internet connection / VPN / SSH during the implementation phase?	Answer 1: No concern; Answer 2: LogRhythm. Answer 3: The assignment has to be completed on site in BCC, so there is no question of providing secure connection over internet.
40	3.1.3	P135	In the Management module will BCC accept implementation of a centralized management server with Virtual Machines for supporting different management applications of the solution?	Clarification required	In the Management module will BCC accept implementation of a centralized management server with Virtual Machines for supporting different management applications of the solution?	Virtualization is acceptable form of delivery, as long as solution matches the requirements.



<b>Subject:</b> Response to Pre-bid Queries (Technical)						
<b>Serial #</b>	<b>Section</b>	<b>Page #</b>	<b>Existing Specification / Condition /Clause</b>	<b>Bidder's Change/ Add/ Delete request</b>	<b>Bidder's Remark</b>	<b>Purchaser's Remark</b>
41	3.1.3	P130		Clarification required	Does BCC have an existing threat intelligence provider supporting the proposed intelligence function? If not, can the bidder propose this capability for either cloud-based or centralized "on premise" threat intelligence services?	BCC has several threat intelligence providers supporting intelligence function. However potential bidders should provide full solution, with relevant threat intelligence capability. Cloud Based Solution is not acceptable.
42	3.1.1.3	P132		Clarification required	In the passive sensor operations, will the sensors be able to incorporate either the cloud-based or on premise the threat intelligence?	The sensors should be able to incorporate on-premise private cloud based threat intelligence. However according to BCC, the sensors are not supposed to have internet connectivity, thus in case cloud is internal to the project, and then it could be implemented during the project.
43	3.1.1.3	P130		Clarification required	In active sensor operations, will BCC allow the bidder to install either a persistent or dissolvable client on the enterprise end-points? Will BCC allow a centralized Vulnerability Management System to access all the enterprise end-points without additional processes?	Answer to both questions is YES. However as sensors will NOT be placed in BCC, so it will be per policy agreed with each organization. All related software and hardware licenses should be included in the Bid Proposal.
44	3.1.1.3	P130		Clarification required	Does BCC have an active patching process and system? If so, can BCC share which system is being used and ability to integrate with vulnerability management systems?	Cannot disclose the details of the BCC security operations. Bid Winner will be informed on the detail existing processes and procedures on signing of a non-disclosure agreement after issuance of notification of award
45	3.1.1.3	P130		Clarification required	Does the Bangladesh government have a networking switching infrastructure at each of the 15 locations that supports 802.1X? Does the Bangladesh government have LDAP or Active Directory fully implemented throughout the enterprise?	Answer to Q1: Almost all the locations support 802.X. Answer to Q2: No.
46	3.1.1.3	P130		Clarification required	Will BCC allow the bidder to install the active sensing mitigation device at each of the locations?	Yes.

<b>Subject: Response to Pre-bid Queries (Technical)</b>						
<b>Serial #</b>	<b>Section</b>	<b>Page #</b>	<b>Existing Specification / Condition /Clause</b>	<b>Bidder's Change/ Add/ Delete request</b>	<b>Bidder's Remark</b>	<b>Purchaser's Remark</b>
47	3.1.1.3	P130		Clarification required	Will the Bangladesh government entertain remote Tier II & III Cyber Analyst Service from a joint venture partner for rules development, event analysis and signatures? Will the Bangladesh government allow secure remote access to the SOC for Tier II & III Cyber Analyst support?	No
48	3.1.1.3	P130		Clarification required	Has BCC considered the addition of malware analysis tools to the passive sensor operations?	Bidder is asked to provide design and is allowed to provide extra capabilities, if they see these capabilities relevant to the technology.
49	3.1.1.3	P130		Clarification required	Does the Bangladesh government have an existing incident handling and processing system? If so, can they share which system is currently in-use?	Bangladesh government is using systems, which are common to incident handling and processing systems, just like other CSIRT teams in many different countries.
50				Clarification required	Will BCC allow "pre-kitting and integration testing of major system components" prior to shipping from a US location?	Yes
51	VII	P131	Supplier has to deploy and integrate incident handling process with BGD e-Gov CIRT processes by using current BGD e-Gov CIRT tools (incident registration tools, integration via API calls to register)	Information required	Question 1: Will you please specify the detailed working principle between the requirement cyber sensor solution and the BDG e-GOV CIRT tools ? Question 2: what kind of features do you expect by doing this ?	Answer to Q1: Cyber sensor after identifying Incident should register this new incident to CIRT incident registration system via email or RESTful API of incident registration tool. Cyber sensor after identifying Incident should register this new incident to CIRT incident registration system via email or RESTful API of incident registration tool. Answer to Q2: Proper functioning, in case of failure, it should report the failure to sensor monitoring system.

Subject: Response to Pre-bid Queries (Technical)						
Serial #	Section	Page #	Existing Specification / Condition /Clause	Bidder's Change/ Add/ Delete request	Bidder's Remark	Purchaser's Remark
52	VII	P132	CSNM must include data tap technology, which would tap at least two links in organization (between internal switch and firewall). Tap component must be able to provide at least two copies of aggregated (i.e. bidirectional traffic placed into one stream, and duplicated on separate port as well) ports. Tap technology must be manageable and configurable via remote secure connection to the device both via GUI as well as via CLI. Taps in at least 13 organizations must tap 1Gbps copper links, and in at least in 2 organizations must tap 10 Gbps links. Link types (fiber single mode/multimode, copper) must be supported and explicitly defined when ordering equipment.	Information required	Here only mentions the physical port of the system. what will be total traffic that the solution will monitor ?	Not more than 10 Gb/second. Total volume of traffic to be monitored cannot be predicted and/or identified at this moment.

Subject: Response to Pre-bid Queries (Technical)						
Serial #	Section	Page #	Existing Specification / Condition / Clause	Bidder's Change/ Add/ Delete request	Bidder's Remark	Purchaser's Remark
53	VII (3.1.3)	from P130 to P135	Detailed Technical Requirements. Item 1, Item 2, Item 3, and Item 4.	Clarification required	Question No. 1: What do you mean Active Sensing capability? Also, is that referring to Vulnerability Analysis tools such as Nessus for items 1 & 2 of that requirement? Question No. 2: In Item 3, it states: "Active sensing via using radar-type technology components (used only in active defense), pre-deployed for emergency and crisis use". Can you clarify this requirement? What do you mean by "radar-type technology" as it relates to sensor operations? Also, it states "CSNM must provide 3 types of sensing:", What is the sensing method of #2 since that is undefined in the document?	There are 3 types of sensing capability requested by BCC. They are as follows: (1) Passive (via copy of traffic – via TAP) – i.e. no interactions possible with client network. (2) Active sensing by honey-pot – it would be connected to client infrastructure, but sit silently. If it will be connected by someone, it will raise alarm (honeypot principle). i.e. interacting with those who are connected, and then alerting owner, but never initiating connections like radar-type. (3) Active sensing – (radar type) "Active sensing" works like active-radar - it emits signals actively, and listens for response. Such mechanism is in tools are like PING, TRACEROUTE, SNMP, etc. There are Open Source tools - like NMAP, OPENVAS – they do assess vulnerabilities, and many other tools are on the market (especially what relates to points 1 and 2), one simple tool is Nessus or its alternatives. Active sensing has to work like advanced radar, i.e. it must emit signal, which will affect the machines (in real life, for example killing the jamming radio signals, electro shocking systems, etc.) . It is required to affect in the way described in #3: When installing the active-sensor (type -3, radar type) capability, it should not be connected to the client network. It should be connected only when client is in crisis. Thereafter the client would ask BCC CIRT for incident assistance, BCC CIRT would then ask – (Please connect red wire into port XX), and then BCC CIRT team could operate active-sensor remotely – for observation, assessment, and other sanctioned operations by the client. Nevertheless, if there is trust between client and BCC, then this capability would always be enabled for active search of vulnerabilities of the network.

Subject: Response to Pre-bid Queries (Procurement Related)						
Serial #	Section	Page #	Existing Specification / Condition /Clause	Bidder's Change/ Add/ Delete request	Bidder's Remark	Purchaser's Remark
54	VII	P137	F. SERVICE SPECIFICATIONS – RECURRENT COST ITEMS, 5.1 Warranty Defect Repair”, the bid documents just mentioned three (3) years warranty.	Are there any requirements about the support & maintenance beyond the three (3) years warranty?	<p><b>F. SERVICE SPECIFICATIONS – RECURRENT COST ITEMS</b></p> <p><b>5.1 Warranty Defect Repair</b></p> <p>5.1.1 The Service MUST provide the following services under the operation of a representative and representative for specified in the bid documents.</p> <p>5.1.1.1 Warranty Defect Repair Services: After (3) years warranty, should provide all components or repairs and materials and software items (hardware) that is required for service. It shall add every maintenance must be factored along with three years for repair and/or labor and parts, on-site and off-site.</p> <p>5.1.1.2 Technical Assistance: Supplier should provide Technical assistance (on-call) post-warranty period. Response time must be less than 2 hours and resolution time must be less than 4 hours.</p> <p><b>Important Note:</b> If items of the above mentioned services shall be included in the cost of the bid/contract price. There will be no separate cost for the items.</p>	Please see "Important Note" in page # 137 of the Request for Bids under section VII (Requirements), subsection F (Service Specifications - Recurrent Costs)
55	2.5 Personnel No:4	P60	Expert in information security and incidence response: Must have minimum 10 years' experience in information security operations and incident response, must have certifications in information security (CISSP, CEH), as well as vendor or independent certification in technical investigation expert (forensics, or cyber security).	We would request you to please modify the clause of proposed manpower as: Must have minimum 5+ years' experience in information security operations and incident response, must have certifications in information security (CISSP, CEH,CISA,ISO 27001,CISM), as well as vendor or independent certification in technical investigation expert (forensics, or cyber security).	None	No Change
56	2.5 Personnel No:6	P60 & P61	Local Cyber Security Expert: Must have experience of operations of dedicated cyber security team, which is working according formal and validated CSIRT processes, a resident of Bangladesh, with minimum 8 years' experience in information security.	We would request you to please modify the clause of proposed manpower as: Must have experience of operations of dedicated cyber security team, which is working according formal and validated CSIRT processes, a resident of Bangladesh, with minimum 4+ years' experience in information security.	None	No Change
57	SECTION II -(BDS), D. Submission and Opening of Bids	P44	The deadline for Bid submission is: Date: 26 April 2017 Time: 15:00 Hours BST (GMT+6 hours)	We request to kindly extend the bid submission date by 21 days from issuance of clarifications and corrigendum of the bid queries.	None	The deadline for bid submission has been changed. Changed submission date is 17 May 2017 15:00 Hours BST (GMT+6)

<b>Subject: Response to Pre-bid Queries (Procurement Related)</b>						
<b>Serial #</b>	<b>Section</b>	<b>Page #</b>	<b>Existing Specification / Condition /Clause</b>	<b>Bidder's Change/ Add/ Delete request</b>	<b>Bidder's Remark</b>	<b>Purchaser's Remark</b>
58	General		Soft copy of forms, tables	Add	Can softcopy of the forms, tables to be used in the RFP response be provided?	Anyone can download the document in PDF from the website <a href="http://www.bcc.gov.bd">http://www.bcc.gov.bd</a> However MS-Word document would be provided only to the bidders who have purchased official bid document.
59	Section 2.7.1.7	P128	Legal expert (1 person)	Information required	What is the scope of work for the legal expert and what has already been done by BCC?	Legal expert should ensure that such sensor deployment and data exchanged is conforming to all international, national, sectorial, organizational, data protection, and national security regulations. If issues arise - this specialist must take leading role in ensuring the resolution of these issues by showing thought leadership and actively working with relevant parties for resolution. There will be a lot of deep data analyzed, legal aspect should be carefully provisioned.
60	Section 2.4.2 Specific Experience	P58	Participation as a prime supplier, management contractor, JV1 member, sub-contractor, in at least one (01) contracts within the last five (05) years, each with a value of at least US\$ 1 million or equivalent amount, that have been successfully and substantially completed and that are similar to the proposed Information System.	Clarification required	Some of the contracts done are extremely confidential due to the nature of organizations for which such work was carried out. In such a situation, what will be the procedure for submitting the proof of such contracts to BCC? Will affidavits from us stating the existence of such contracts suffice?	Affidavit by the Bidders certified by a notary public regarding existence of such contracts will do, in absence of certification from the client directly due to security/ policy reason. However, during post-qualification of the successful bidder, claim against this criterion will be verified from the source and the concern Bidder has to produce necessary documents and contacts at that time.

<b>Subject: Response to Pre-bid Queries (Procurement Related)</b>						
<b>Serial #</b>	<b>Section</b>	<b>Page #</b>	<b>Existing Specification / Condition /Clause</b>	<b>Bidder's Change/ Add/ Delete request</b>	<b>Bidder's Remark</b>	<b>Purchaser's Remark</b>
61	General		Taxation	Clarification required	Please help us understanding tax heads and prevailing rates applicable to national and international companies, participating in this bid	According to the rules and regulations of the Government of Bangladesh. However for bid preparation please follow Section 1 - Instruction to Bidders (ITB), Clause 17. Bid Price including all subclauses under clause 17 ( from page # 19 to page # 21) and also clause 18. Currencies of Bid and Payment (in page # 22).
62	Sec I- ITB 4. Eligible Bidders 4.1; Sec II BDS	P9 and P40	It is preferable to limit maximum 3 members in the JV.	Information required	From the term 'preferable ' statement we assume that no JV members can be more than 3.	More than three members in a JV is allowed.
63	IV	P69	3.2 Supply and Installation Cost Summary Table	As our offered solution may contain multiple subcomponents in one subsystem/item we would like to include additional row or column with and number them like 2.1, 2.2 under Cyber Sensor Management Module or 3.1, 3.2 under Cyber Sensor Network Module. Please suggest.	Without adding subcomponent as one subsystem may have many, there can be ambiguity in offer.	If required then please include additional row and/or column, however you should maintain the serial structure of the table.
64	IV	P71	3.4 Supply and Installation Cost Summary Table	As our offered solution may contain multiple subcomponents in one subsystem/item we would like to include additional row or column with and number them like 2.1, 2.2 under Cyber Sensor Management Module or 3.1, 3.2 under Cyber Sensor Network Module. Please suggest.	Without adding subcomponent as one subsystem may have many, there can be ambiguity in offer.	If required then please include additional row and/or column, however you should maintain the serial structure of the table.