Request for Bids

Information Systems

Design, Supply and Installation
(One-Envelope Bidding Process)

Procurement of:

Supply, Installation and Commissioning of Hardware & Software for Establishment of Cyber Defense Training Center at BCC

……

RFB No: Contract Package # AF-G5

Project: Leveraging ICT for Growth, Employment & Governance Project

Employer: Bangladesh Computer Council (BCC)

Information and Communication Technology Division

Ministry of Posts, Telecommunications and Information Technology

Country: Bangladesh

Issued on: 07 August 2017

Request for Bid
Information Systems
(Design, Supply and Installation)

Memo No.: 56.109.007.0000.065.2017-83 Date: August 07, 2017

Purchaser: Bangladesh Computer Council (BCC)

Project: Leveraging ICT for Growth, Employment & Governance Project

Contract title: Supply, Installation and Commissioning of Hardware & Software for Establishment of Cyber Defense Training Center at BCC

Country: *Bangladesh*

Credit No.: *5911-BD*

RFB No: *AF-G5*

Issued on: *07 August 2017*

1. The People's Republic of Bangladesh has received financing from the World Bank toward the cost of the Leveraging ICT for Growth, Employment & Governance Project and intends to apply part of the proceeds toward payments under the contract for Supply, Installation and Commissioning of Hardware & Software for Establishment of Cyber Defense Training Center at BCC.

2. The Bangladesh Computer Council (BCC) represented by the Project Director, Leveraging ICT for Growth, Employment & Governance Project now invites sealed Bids from eligible Bidders for Supply, Installation and Commissioning of Hardware & Software for Establishment of Cyber Defense Training Center at BCC.

3. Bidding will be conducted through international competitive procurement using Request for Bids (RFB) as specified in the World Bank's "Procurement Regulations for IPF Borrowers" *July 2016* ("Procurement Regulations"), and is open to all eligible Bidders as defined in the Procurement Regulations.

4. Interested eligible Bidders may obtain further information from Project Director, Leveraging ICT for Growth, Employment and Governance Project, ICT Tower, Plot # E-14/X, Agargaon, Sher-e-Bangla Nagar, Dhaka -1207, Bangladesh. For the convenience of the Bidders an unofficial electronic copy of bidding document can also be viewed at website www.bcc.gov.bd (for inspection purpose only).

5. The bidding document (official hard copy) in ***English*** may be purchased by interested eligible Bidders upon the submission of a written application to the address below and upon payment of a nonrefundable fee of Bangladesh Taka (BDT) 6,000 (BDT Six Thousand only) or in US$ 75 (US$ Seventy Five only). The method of payment will be Bank Draft or Pay Order in favor of Project Director, Leveraging ICT for Growth, Employment and Governance Project. For overseas delivery, the bidder may obtain the bidding document by

instructing any international courier service to collect the same from Project Director, Leveraging ICT for Growth, Employment and Governance Project, ICT Tower, Plot # E-14/X, Agargaon, Sher-e-Bangla Nagar, Dhaka -1207, Bangladesh.

6. Bids must be delivered to the address below on or before 09 October 2017 up to BST 15:00 hours (GMT+6 hours). Electronic Bidding will not be permitted. Late Bids will be rejected. Bids will be publicly opened in the presence of the Bidders' designated representatives and anyone who chooses to attend at the address below on BST 15:30 hours (GMT +6:00 hours) on 09 October 2017.

7. All Bids shall be valid for a period of 150 days after bid closing and must be accompanied by bid security of United States Dollar (US$) 25,000 (US$ Twenty Five Thousand only) or BDT 2,000,000 (BDT Two Million Only) or an equivalent amount in a freely convertible currency.

8. A Pre-bid meeting with the representatives of prospective bidders will be held at the address below at BST 11: 00 hours (BST= GMT + 6:00 hours) on 11 September 2017.

9. The attention of prospective Bidders is drawn to (i) the fact that they will be required to certify in their bids that all software is either covered by a valid license or was produced by the Bidder and (ii) that violations are considered fraud, which can result in ineligibility to be awarded World Bank-financed contracts.

10. The authority reserves the right to accept or reject any or all bids without assigning any reason thereof.

Project Director
Leveraging ICT for Growth, Employment and Governance Project
Bangladesh Computer Council (BCC), ICT Tower (2nd Floor),
Plot # E-14/X, Agargaon, Sher-e-Bangla Nagar, Dhaka -1207, Bangladesh.
Telephone: +880-2-8181381, Fax: +880-2-8181383
E-mail: pd.lict@bcc.net.bd

Table of Contents

PART 1 – BIDDING PROCEDURES

SECTION I - INSTRUCTIONS TO BIDDERS (ITB)

Contents

Section I - Instructions to Bidders

A. GENERAL

1. Scope of Bid

1.1 The Purchaser, as indicated **in the BDS**, or its duly authorized Purchasing Agent if so specified **in the BDS** (interchangeably referred to as "the Purchaser" issues this bidding document for the supply and installation of the Information System as specified in Section VII, Purchaser's Requirements. The name, identification and number of lots (contracts) of this RFB are specified **in the BDS.**

1.2 Unless otherwise stated, throughout this bidding document definitions and interpretations shall be as prescribed in the Section VIII, General Conditions of Contract.

1.3 Throughout this bidding document:

(a) the term "in writing" means communicated in written form (e.g. by mail, e-mail, fax, including if specified **in the BDS**, distributed or received through the electronic-procurement system used by the Purchaser) with proof of receipt;

(b) if the context so requires, "singular" means "plural" and vice versa; and

(c) "Day" means calendar day, unless otherwise specified as "Business Day". A Business Day is any day that is an official working day of the Borrower. It excludes the Borrower's official public holidays.

2. Source of Funds

2.1 The Borrower or Recipient (hereinafter called "Borrower") indicated **in the BDS** has applied for or received financing (hereinafter called "funds") from the International Bank for Reconstruction and Development or the International Development Association (hereinafter called "the Bank") in an amount specified **in the BDS** toward the project named **in the BDS**. The Borrower intends to apply a portion of the funds to eligible payments under the contract(s) for which this bidding document is issued.

2.2 Payments by the Bank will be made only at the request of the Borrower and upon approval by the Bank in accordance with the terms and conditions of the Loan (or other financing) Agreement between the Borrower and the Bank (hereinafter called the Loan Agreement), and will be subject in all respects to the terms and conditions of that Loan (or other financing) Agreement. The Loan (or other financing) Agreement prohibits a withdrawal from the loan account for the purpose of any payment to persons or entities, or for any import of equipment, materials or any other goods, if such payment or import is prohibited by a decision of the United Nations Security Council taken under Chapter VII of the Charter of the United Nations. No party other than the Borrower shall derive any rights from the Loan (or other financing) Agreement or have any claim to the funds.

3. Fraud and Corruption

3.1 The Bank requires compliance with the Bank's Anti-Corruption Guidelines and its prevailing sanctions policies and procedures as set forth in the WBG's Sanctions Framework, as set forth in Section VI.

3.2 In further pursuance of this policy, Bidders shall permit and shall cause its agents (where declared or not), subcontractors, sub consultants, service providers, suppliers, and their personnel, to permit the Bank to inspect all accounts, records and other documents relating to any initial selection process, prequalification process, bid submission, proposal submission and contract performance (in the case of award), and to have them audited by auditors appointed by the Bank.

4. Eligible Bidders

4.1 A Bidder may be a firm that is a private entity, a state-owned enterprise or institution subject to ITB 4.6, or any combination of such entities in the form of a joint venture (JV) under an existing agreement or with the intent to enter into such an agreement supported by a letter of intent. In the case of a joint venture, all members shall be jointly and severally liable for the execution of the Contract in accordance with the Contract terms. The JV shall nominate a Representative who shall have the authority to conduct all business for and on behalf of any

and all the members of the JV during the Bidding process and, in the event the JV is awarded the Contract, during contract execution. Unless specified **in the BDS**, there is no limit on the number of members in a JV.

4.2 A Bidder shall not have a conflict of interest. Any Bidder found to have a conflict of interest shall be disqualified. A Bidder may be considered to have a conflict of interest for the purpose of this Bidding process, if the Bidder:

(a) Directly or indirectly controls, is controlled by or is under common control with another Bidder; or

(b) Receives or has received any direct or indirect subsidy from another Bidder; or

(c) Has the same legal representative as another Bidder; or

(d) Has a relationship with another Bidder, directly or through common third parties, that puts it in a position to influence the Bid of another Bidder, or influence the decisions of the Purchaser regarding this Bidding process; or

(e) Any of its affiliates participates as a consultant in the preparation of the design or technical specifications of the Information System that are the subject of the Bid; or

(f) or any of its affiliates has been hired (or is proposed to be hired) by the Purchaser or Borrower as Project Manager for the Contract implementation; or

(g) would be providing goods, works, or non-consulting services resulting from or directly related to consulting services for the preparation or implementation of the project specified in the BDS ITB 2.1 that it provided or were provided by any affiliate that directly or indirectly controls, is controlled by, or is under common control with that firm; or

(h) has a close business or family relationship with a professional staff of the Borrower (or of the project implementing agency, or of a recipient of a part of the loan) who: (i) are directly or indirectly involved in the preparation of the bidding document or specifications of the Contract, and/or the Bid evaluation process of such Contract; or (ii) would be involved in the

implementation or supervision of such Contract unless the conflict stemming from such relationship has been resolved in a manner acceptable to the Bank throughout the Bidding process and execution of the Contract.

4.3 A firm that is a Bidder (either individually or as a JV member) shall not participate as a Bidder or as JV member in more than one Bid except for permitted alternative Bids. Such participation shall result in the disqualification of all Bids in which the firm is involved. However, this does not limit the participation of a Bidder as subcontractor in another Bid or of a firm as a subcontractor in more than one Bid.

4.4 A Bidder may have the nationality of any country, subject to the restrictions pursuant to ITB 4.8. A Bidder shall be deemed to have the nationality of a country if the Bidder is constituted, incorporated or registered in and operates in conformity with the provisions of the laws of that country, as evidenced by its articles of incorporation (or equivalent documents of constitution or association) and its registration documents, as the case may be. This criterion also shall apply to the determination of the nationality of proposed sub-contractors or sub-consultants for any part of the Contract including related Services.

4.5 A Bidder that has been sanctioned by the Bank, pursuant to the Bank's Anti-Corruption Guidelines, and in accordance with its prevailing sanctions policies and procedures as set forth in the WBG's Sanctions Framework as described in Section VI paragraph 2.2 d., shall be ineligible to be initially selected for, prequalified for, bid for, submit proposal for, or be awarded a Bank-financed contract or benefit from a Bank-financed contract, financially or otherwise, during such period of time as the Bank shall have determined. The list of debarred firms and individuals is available at the electronic address specified in the BDS.

4.6 Bidders that are state-owned enterprises or institutions in the Purchaser's Country may be eligible to compete and be awarded a Contract(s) only if they can establish, in a manner acceptable to the Bank, that they (i) are legally and financially autonomous (ii) operate under commercial law, and (iii) are not under supervision of the Purchaser.

4.7 A Bidder shall not be under suspension from bidding/submitting proposals by the Purchaser as the result of the operation of a

Bid–Securing Declaration.

4.8 Firms and individuals may be ineligible if so indicated in Section V and (a) as a matter of law or official regulations, the Borrower's country prohibits commercial relations with that country, provided that the Bank is satisfied that such exclusion does not preclude effective competition for the supply of goods or the contracting of works or services required; or (b) by an act of compliance with a decision of the United Nations Security Council taken under Chapter VII of the Charter of the United Nations, the Borrower's country prohibits any import of goods or contracting of works or services from that country, or any payments to any country, person, or entity in that country.

4.9 This Bidding is open for all eligible Bidders, unless otherwise specified in ITB 15.2.

4.10 A Bidder shall provide such documentary evidence of eligibility satisfactory to the Purchaser, as the Purchaser shall reasonably request.

4.11 A firm that is under a sanction of debarment by the Borrower from being awarded a contract is eligible to participate in this procurement, unless the Bank, at the Borrower's request, is satisfied that the debarment; (a) relates to fraud or corruption, and (b) followed a judicial or administrative proceeding that afforded the firm adequate due process.

5. Eligible Goods and Services

5.1 The Information Systems to be supplied under the Contract and financed by the Bank may have their origin in any country in accordance with Section V, Eligible Countries.

5.2 For the purposes of this bidding document, the term "Information System" means all:

(a) the required information technologies, including all information processing and communications-related hardware, software, supplies, and consumable items that the Supplier is required to supply and install under the Contract, plus all associated documentation, and all other materials and goods to be supplied, installed, integrated, and made operational; and

(b) the related software development, transportation, insurance, installation, customization, integration, commissioning, training, technical support, maintenance, repair, and other services necessary for proper operation of the Information System to be provided by the selected Bidder and as specified in the Contract.

5.3 For purposes of ITB 5.1 above, "origin" means the place where the goods and services making the Information System are produced in or supplied from. An Information System is deemed to be produced in a certain country when, in the territory of that country, through software development, manufacturing, or substantial and major assembly or integration of components, a commercially recognized product results that is substantially different in basic characteristics or in purpose or utility from its components.

B. CONTENTS OF BIDDING DOCUMENT

6. Sections of Bidding Document

6.1 The bidding document consists of Parts 1, 2, and 3, which include all the sections indicated below, and should be read in conjunction with any Addenda issued in accordance with ITB 8:

PART 1 - Bidding Procedures

Section I - Instructions to Bidders (ITB)

Section II - Bid Data Sheet (BDS)

Section III - Evaluation and Qualification Criteria

Section IV - Bidding Forms

Section V - Eligible Countries

Section VI - Fraud and Corruption

PART 2 - Purchaser's Requirements

Section VII - Requirements of the IS, including:

- Technical Requirements
- Implementation Schedule
- System Inventory Tables
- Background and Informational Materials

PART 3 - Contract

Section VIII - General Conditions of Contract

Section IX -Special Conditions of Contract

Section X - Contract Forms

6.2 The Specific Procurement Notice – Request for Bids (RFB) issued by the Purchaser is not part of this bidding document.

6.3 Unless obtained directly from the Purchaser, the Purchaser is not responsible for the completeness of the document, responses to requests for clarification, the Minutes of the pre-Bid meeting (if any), or Addenda to the bidding document in accordance with ITB 8. In case of any contradiction, documents obtained directly from the Purchaser shall prevail.

6.4 The Bidder is expected to examine all instructions, forms, terms, and specifications in the bidding document and to furnish with its Bid all information or documentation as is required by the bidding document.

7. Clarification of Bidding Document, Site Visit, Pre-bid Meeting

7.1 A Bidder requiring any clarification of the bidding document shall contact the Purchaser in writing at the Purchaser's address specified **in the BDS** or raise its enquiries during the pre-Bid meeting if provided for in accordance with ITB 7.4. The Purchaser will respond in writing to any request for clarification, provided that such request is received prior to the deadline for submission of Bids within a period specified **in the BDS.** The Purchaser's shall forward copies of its response to all Bidders who have acquired the bidding document in accordance with ITB 6.3, including a description of the inquiry but without identifying its source. If so specified **in the BDS**, the Purchaser shall also promptly publish its response at the web page identified **in the BDS**. Should the Purchaser deem it necessary to amend the bidding document as a result of a request for clarification, it shall do so following the procedure under ITB 8 and ITB 23.2.

7.2 The Bidder may wish to visit and examine the site where the Information System is to be installed and its surroundings and obtain for itself on its own responsibility all information that may be necessary for preparing the Bid and entering into a contract. The costs of visiting the site shall be at the Bidder's own expense.

7.3 The Bidder and any of its personnel or agents will be granted permission by the Purchaser to enter upon its premises and lands for the purpose of such visit, but only upon the express condition that the Bidder, its personnel, and agents will release and indemnify the Purchaser and its personnel and agents from and against all liability in respect thereof, and will be responsible for death or personal injury, loss of or damage to property, and any other loss, damage, costs, and expenses incurred as a result of the inspection.

7.4 The Bidder's designated representative is invited to attend a pre-Bid meeting and/or a site visit, if provided for **in the BDS**. The purpose of the meeting will be to clarify issues and to answer questions on any matter that may be raised at that stage.

7.5 The Bidder is requested, as far as possible, to submit any questions in writing, to reach the Purchaser not later than one week before the meeting.

7.6 Minutes of the pre-Bid meeting, including the text of the questions raised without identifying the source, and the responses given, together with any responses prepared after the meeting, will be transmitted promptly to all Bidders who have acquired the bidding document in accordance with ITB 6.3. Any modification to the bidding document that may become necessary as a result of the pre-Bid meeting shall be made by the Purchaser exclusively through the issue of an Addendum pursuant to ITB 8 and not through the minutes of the pre-Bid meeting.

7.7 Nonattendance at the pre-Bid meeting will not be a cause for disqualification of a Bidder.

8. Amendment of Bidding Document

8.1 At any time prior to the deadline for submission of Bids, the Purchaser may amend the bidding document by issuing addenda.

8.2 Any addendum issued shall be part of the bidding document and shall be communicated in writing to all who have obtained the bidding document from the Purchaser in accordance with ITB 6.3. The Purchaser shall also promptly publish the addendum on the Purchaser's web page in accordance with ITB 7.1.

8.3 To give prospective Bidders reasonable time in which to take an addendum into account in preparing their Bids, the Purchaser may, at its discretion, extend the deadline for the submission of Bids, pursuant to ITB 23.2

C. PREPARATION OF BIDS

9. Cost of Bidding

9.1 The Bidder shall bear all costs associated with the preparation and submission of its Bid, and the Purchaser shall not be responsible or liable for those costs, regardless of the conduct or outcome of the Bidding process.

10. Language of Bid

10.1 The Bid, as well as all correspondence and documents relating to the bid exchanged by the Bidder and the Purchaser, shall be written in the language specified **in the BDS.** Supporting documents and printed literature that are part of the Bid may be in another language provided they are accompanied by an accurate translation of the relevant passages in the language specified **in the BDS**, in which case, for purposes of interpretation of the Bid, such translation shall govern.

11. Documents Comprising the Bid

11.1 The Bid submitted by the Bidder shall comprise the following:

(a) **Letter of Bid** prepared in accordance with ITB 12;

(b) **Price Schedules** completed in accordance with ITB 12 and ITB 17;

(c) **Bid Security or Bid-Securing Declaration** in accordance with ITB 20;

(d) **Alternative Bid:** if permissible, in accordance with ITB 13;

(e) **Authorization:** written confirmation authorizing the signatory of the Bid to commit the Bidder, in accordance with ITB 21.3;

(f) **Eligibility of Information System:** documentary evidence established in accordance with ITB 14.1 that the Information System offered by the Bidder in its Bid or in any alternative Bid, if permitted, are eligible;

(g) **Bidder's Eligibility:** documentary evidence in accordance with ITB 15 establishing the Bidder's eligibility and qualifications to perform the contract if its Bid is accepted;

(h) **Conformity:** documentary evidence established in accordance with ITB 16 that the Information System offered by the Bidder conform to the bidding document;

(i) **Subcontractors:** list of subcontractors, in accordance with ITB 16.4;

(j) **Intellectual Property**: a list of: Intellectual Property as defined in GCC Clause 15;

(i) all Software included in the Bid, assigning each item to one of the software categories defined in GCC Clause 1.1 (c):

a. System, General Purpose, and Application Software; or

b. Standard and Custom Software;

(ii) all Custom Materials, as defined in GCC Clause 1.1 (c), included in the Bid;

All Materials not identified as Custom Materials shall be deemed Standard Materials, as defined in GCC Clause 1.1 (c);

Re-assignments among the Software and Materials categories, if necessary, will be made during the implementation of the Contract according to GCC Clause 39 (Changes to the Information System); and

(k) any other document required **in the BDS.**

11.2 In addition to the requirements under ITB 11.1, Bids submitted by a JV shall include a copy of the Joint Venture Agreement entered into by all members indicating at least the parts of the Information System to be executed by the respective members. Alternatively, a letter of intent to execute a Joint Venture Agreement in the event of a successful Bid shall be signed by all members and submitted with the Bid, together with a copy

of the proposed Agreement indicating at least the parts of the Information System to be executed by the respective members.

11.3 The Bidder shall furnish in the Letter of Bid information on commissions and gratuities, if any, paid or to be paid to agents or any other party relating to this Bid.

12. Letter of Bid and Price Schedules

12.1 The Bidder shall complete the Letter of Bid, including the appropriate Price Schedules, using the relevant forms furnished in Section IV, Bidding Forms. The forms must be completed without any alterations to the text, and no substitutes shall be accepted except as provided under ITB 21.3. All blank spaces shall be filled in with the information requested.

13. Alternative Bids

13.1 The BDS indicates whether alternative Bids are allowed. If they are allowed, the **BDS** will also indicate whether they are permitted in accordance with ITB 13.3, or invited in accordance with ITB 13.2 and/or ITB 13.4.

13.2 When alternatives to the Time Schedule are explicitly invited, a statement to that effect will be included **in the BDS**, and the method of evaluating different time schedules will be described in Section III, Evaluation and Qualification Criteria.

13.3 Except as provided under ITB 13.4 below, Bidders wishing to offer technical alternatives to the Purchaser's requirements as described in the bidding document must also provide: (i) a price at which they are prepared to offer an Information System meeting the Purchaser's requirements; and (ii) all information necessary for a complete evaluation of the alternatives by the Purchaser, including drawings, design calculations, technical specifications, breakdown of prices, and proposed installation methodology and other relevant details. Only the technical alternatives, if any, of the Bidder with the Most Advantageous Bid conforming to the basic technical requirements shall be considered by the Purchaser.

13.4 When Bidders are invited **in the BDS** to submit alternative technical solutions for specified parts of the system, such parts shall be described in Section VII, Purchaser's Requirements. Technical alternatives that comply with the performance and technical criteria specified for the Information System shall be considered by the Purchaser on their own merits, pursuant to ITB 35.

14. Documents Establishing the

14.1 To establish the eligibility of the Information System in accordance with ITB 5, Bidders shall complete the country of

Eligibility of the Information System

origin declarations in the Price Schedule Forms, included in Section IV, Bidding Forms.

15. Documents Establishing the Eligibility and Qualifications of the Bidder

15.1 To establish its eligibility and qualifications to perform the Contract in accordance with Section III, Evaluation and Qualification Criteria, the Bidder shall provide the information requested in the corresponding information sheets included in Section IV, Bidding Forms.

15.2 In the event that prequalification of potential Bidders has been undertaken as stated **in the BDS**, only Bids from prequalified Bidders shall be considered for award of Contract. These qualified Bidders should submit with their Bids any information updating their original prequalification applications or, alternatively, confirm in their Bids that the originally submitted prequalification information remains essentially correct as of the date of Bid submission.

16. Documents Establishing Conformity of the Information System

16.1 Pursuant to ITB 11.1 (h), the Bidder shall furnish, as part of its Bid documents establishing the conformity to the bidding documents of the Information System that the Bidder proposes to design, supply and install under the Contract

16.2 The documentary evidence of conformity of the Information System to the bidding documents including:

(a) Preliminary Project Plan describing, among other things, the methods by which the Bidder will carry out its overall management and coordination responsibilities if awarded the Contract, and the human and other resources the Bidder proposes to use. The Preliminary Project Plan must also address any other topics **specified in the BDS**. In addition, the Preliminary Project Plan should state the Bidder's assessment of what it expects the Purchaser and any other party involved in the implementation of the Information System to provide during implementation and how the Bidder proposes to coordinate the activities of all involved parties;

(b) written confirmation that the Bidder accepts responsibility for the successful integration and inter-operability of all components of the Information System as required by the bidding documents;

(c) An item-by-item commentary on the Purchaser's Technical Requirements, demonstrating the substantial responsiveness of the Information System offered to

those requirements. In demonstrating responsiveness, the Bidder is encouraged to use the Technical Responsiveness Checklist (or Checklist Format) in the Sample Bidding Forms (Section IV). The commentary shall include explicit cross-references to the relevant pages in the supporting materials included in the bid. Whenever a discrepancy arises between the item-by-item commentary and any catalogs, technical specifications, or other preprinted materials submitted with the bid, the item-by-item commentary shall prevail;

(d) support material (e.g., product literature, white papers, narrative descriptions of technologies and/or technical approaches), as required and appropriate; and

(e) Any separate and enforceable contract(s) for Recurrent Cost items which the BDS ITB 17.2 required Bidders to bid.

16.3 References to brand names or model numbers or national or proprietary standards designated by the Purchaser in the bidding documents are intended to be descriptive and not restrictive. Except where explicitly **prohibited in the BDS** for specific items or standards, the Bidder may substitute alternative brand/model names or standards in its bid, provided that it demonstrates to the Purchaser's satisfaction that the use of the substitute(s) will result in the Information System being able to perform substantially equivalent to or better than that specified in the Technical Requirements.

16.4 For major items of the Information System as listed by the Purchaser in Section III, Evaluation and Qualification Criteria, which the Bidder intends to purchase or subcontract, the Bidder shall give details of the name and nationality of the proposed subcontractors, including manufacturers, for each of those items. In addition, the Bidder shall include in its Bid information establishing compliance with the requirements specified by the Purchaser for these items. Quoted rates and prices will be deemed to apply to whichever subcontractor is appointed, and no adjustment of the rates and prices will be permitted.

16.5 The Bidder shall be responsible for ensuring that any subcontractor proposed complies with the requirements of ITB 4, and that any goods or services to be provided by the subcontractor comply with the requirements of ITB 5 and ITB 16.1.

17. Bid Prices

17.1 All Goods and Services identified in the Supply and Installation Cost Sub-Tables in System Inventory Tables in Section VII, and all other Goods and Services proposed by the Bidder to fulfill the requirements of the Information System, must be priced separately and summarized in the corresponding cost tables in the Sample Bidding Forms (Section IV), in accordance with the instructions provided in the tables and in the manner specified below.

17.2 **Unless otherwise specified in the BDS**, the Bidder must also bid Recurrent Cost Items specified in the Technical Requirements, Recurrent Cost Sub-Table of the System Inventory Tables in Section VII (if any). These must be priced separately and summarized in the corresponding cost tables in the Sample Bidding Forms (Section IV), in accordance with the instructions provided in the tables and in the manner specified below:

(a) **if specified in the BDS,** the Bidder must also bid separate enforceable contracts for the Recurrent Cost Items not included in the main Contract;

(b) prices for Recurrent Costs are all-inclusive of the costs of necessary Goods such as spare parts, software license renewals, labor, etc., needed for the continued and proper operation of the Information System and, if appropriate, of the Bidder's own allowance for price increases;

(c) Prices for Recurrent Costs beyond the scope of warranty services to be incurred during the Warranty Period, defined in GCC Clause 29.4 and prices for Recurrent Costs to be incurred during the Post-Warranty Period, defined in SCC Clause 1.1. (e) (xiii), shall be quoted as Service prices on the Recurrent Cost Sub-Table in detail, and on the Recurrent Cost Summary Table in currency totals.

17.3 Unit prices must be quoted at a level of detail appropriate for calculation of any partial deliveries or partial payments under the contract, in accordance with the Implementation Schedule in Section VII), and with GCC and SCC Clause 12 – Terms of Payment. Bidders may be required to provide a breakdown of any composite or lump-sum items included in the Cost Tables

17.4 The price of items that the Bidder has left blank in the cost tables provided in the Sample Bid Forms (Section IV) shall

be assumed to be included in the price of other items. Items omitted altogether from the cost tables shall be assumed to be omitted from the bid and, provided that the bid is substantially responsive, an adjustment to the bid price will be made during bid evaluation in accordance with ITB 31.3.

17.5 The prices for Goods components of the Information System are to be expressed and shall be defined and governed in accordance with the rules prescribed in the edition of Incoterms **specified in the BDS,** as follows:

(a) Goods supplied from outside the Purchaser's country:

Unless otherwise specified in the BDS, the prices shall be quoted on a CIP (named place of destination) basis, exclusive of all taxes, stamps, duties, levies, and fees imposed in the Purchaser's country. The named place of destination and special instructions for the contract of carriage are as specified in the SCC for GCC 1.1 (e) (iii)**.** In quoting the price, the Bidder shall be free to use transportation through carriers registered in any eligible countries. Similarly, the Bidder may obtain insurance services from any eligible source country;

(b) Locally supplied Goods:

Unit prices of Goods offered from within the Purchaser's Country, shall be quoted on an EXW (ex factory, ex works, ex warehouse or off-the-shelf, as applicable) basis, including all customs duties, levies, fees, sales and other taxes incurred until delivery of the Goods, but excluding all VAT or sales and other taxes and duties/fees incurred for the Goods at the time of invoicing or sales transaction, if the Contract is awarded;

(c) Inland transportation.

17.6 **Unless otherwise stated in the BDS**, inland transportation, insurance and related local costs incidental to the delivery of the Goods to the designated Project Sites must be quoted separately as a Service item in accordance with ITB 17.5, whether the Goods are to be supplied locally or from outside the Purchaser's country, except when these costs are already included in the price of the Goods, as is, e.g., the case, when ITB 17.5 (a) specifies CIP, and the named places of destination are the Project Sites.

17.7 The price of Services shall be separated into their local and foreign currency components and where appropriate, broken

down into unit prices. Prices must include all taxes, duties, levies and fees whatsoever, except only VAT or other indirect taxes, or stamp duties, that may be assessed and/or apply in the Purchaser's country on/to the price of the Services invoiced to the Purchaser, if the Contract is awarded.

17.8 **Unless otherwise specified in the BDS,** the prices must include all costs incidental to the performance of the Services, as incurred by the Supplier, such as travel, subsistence, office support, communications, translation, printing of materials, etc. Costs incidental to the delivery of the Services but incurred by the Purchaser or its staff, or by third parties, must be included in the price only to the extent such obligations are made explicit in these bidding documents (as, e.g., a requirement for the Bidder to include the travel and subsistence costs of trainees).

17.9 **Unless otherwise specified in the BDS,** prices quoted by the Bidder shall be fixed during the Bidder's performance of the Contract and not subject to increases on any account. Bids submitted that are subject to price adjustment will be rejected.

18. Currencies of Bid and Payment

18.1 The currency (ies) of the Bid and currencies of payment shall be the same. The Bidder shall quote in the currency of the Purchaser's Country the portion of the Bid price that corresponds to expenditures incurred in the currency of the Purchaser's Country, unless otherwise specified **in the BDS**.

18.2 The Bidder may express the Bid price in any currency. If the Bidder wishes to be paid in a combination of amounts in different currencies, it may quote its price accordingly but shall use no more than three foreign currencies in addition to the currency of the Purchaser's Country.

19. Period of Validity of Bids

19.1 Bids shall remain valid for the period specified **in the BDS** after the Bid submission deadline date prescribed by the Purchaser in accordance with ITB 23.1. A Bid valid for a shorter period shall be rejected by the Purchaser as nonresponsive.

19.2 In exceptional circumstances, prior to the expiration of the Bid validity period, the Purchaser may request Bidders to extend the period of validity of their Bids. The request and the responses shall be made in writing. If a Bid Security is requested in accordance with ITB 20.1, it shall also be extended for twenty-eight days (28) beyond the deadline of the extended validity period. A Bidder may refuse the request without forfeiting its Bid Security. A Bidder granting the request shall not be required or permitted to modify its Bid, except as provided in ITB 19.3.

19.3 If the award is delayed by a period exceeding fifty-six (56) days beyond the expiry of the initial Bid validity, the Contract price shall be determined as follows:

(a) in case of fixed price contracts, the contract price shall be the Bid price adjusted by a factor or factors specified **in the BDS**;

(b) in the case of an adjustable price contracts, no adjustments shall be made;

(c) In any case, Bid evaluation shall be based on the Bid Price without taking into consideration the applicable correction from those indicated above.

20. Bid Security

20.1 The Bidder shall furnish as part of its Bid, either a Bid-Securing Declaration or a Bid Security as specified **in the BDS**, in original form and, in the case of a Bid Security, in the amount and currency specified **in the BDS**.

20.2 A Bid-Securing Declaration shall use the form included in Section IV, Bidding Forms.

20.3 If a Bid Security is specified pursuant to ITB 20.1, the bid security shall be a demand guarantee in any of the following forms at the Bidder's option:

(a) an unconditional guarantee issued by a non-bank financial institution (such as an insurance, bonding or surety company);

(b) an irrevocable letter of credit;

(c) a cashier's or certified check; or

(d) another security indicated **in the BDS,**

From a reputable source from an eligible country. If an unconditional guarantee is issued by a non-bank financial institution located outside the Purchaser's Country the issuing non-bank financial institution shall have a correspondent financial institution located in the Purchaser's Country to make it enforceable unless the Purchaser has agreed in writing, prior to Bid submission, that a correspondent financial institution is not required.

20.4 In the case of a bank guarantee, the Bid Security shall be submitted either using the Bid Security Form included in Section IV, Bidding Forms or in another substantially similar format approved by the Purchaser prior to Bid submission. In either case, the form must include the complete name of the Bidder. The Bid Security shall be valid for twenty-eight days (28) beyond the original validity period of the Bid, or beyond any period of extension if requested under ITB 19.2.

20.5 If a Bid Security or a Bid-Securing Declaration is specified pursuant to ITB 20.1, any Bid not accompanied by a substantially responsive Bid Security or Bid-Securing Declaration shall be rejected by the Purchaser as non-responsive.

20.6 If a Bid Security is specified pursuant to ITB 20.1, the Bid Security of unsuccessful Bidders shall be returned as promptly as possible upon the successful Bidder's furnishing of the Performance Security pursuant to ITB 47.

20.7 The Bid Security of the successful Bidder shall be returned as promptly as possible once the successful Bidder has signed the Contract and furnished the required Performance Security.

20.8 The Bid Security may be forfeited or the Bid-Securing Declaration executed:

(a) if a Bidder withdraws its Bid during the period of Bid validity specified by the Bidder on the Letter of Bid; or

(b) if the successful Bidder fails to**:**

(i) Sign the Contract in accordance with ITB 46; or

(ii) Furnish a performance security in accordance with ITB 47.

20.9 The Bid Security or the Bid-Securing Declaration of a JV shall be in the name of the JV that submits the bid. If the JV has not been legally constituted into a legally enforceable JV at the time of Bidding, the Bid Security or the Bid-Securing Declaration shall be in the names of all future members as named in the letter of intent referred to in ITB 4.1 and ITB 11.2.

20.10 If a Bid Security is not required **in the BDS**, and;

(a) if a Bidder withdraws its Bid during the period of Bid validity specified by the Bidder on the Letter of Bid Form, except as provided in ITB 19.2; or

(b) if the successful Bidder fails to: sign the Contract in accordance with ITB 46; or furnish a Performance Security in accordance with ITB 47;

the Purchaser may, if provided for **in the BDS**, declare the Bidder disqualified to be awarded a contract by the Purchaser for a period of time as stated **in the BDS**.

21. Format and Signing of Bid

21.1 The Bidder shall prepare one original of the documents comprising the Bid as described in ITB 11 and clearly mark it "ORIGINAL." Alternative Bids, if permitted in accordance with ITB 13, shall be clearly marked "ALTERNATIVE". In addition, the Bidder shall submit copies of the Bid, in the number specified **in the BDS** and clearly mark them "COPY." In the event of any discrepancy between the original and the copies, the original shall prevail.

21.2 Bidders shall mark as "CONFIDENTIAL" information in their Bids which is confidential to their business. This may include proprietary information, trade secrets, or commercial or financially sensitive information.

21.3 The original and all copies of the Bid shall be typed or written in indelible ink and shall be signed by a person duly authorized to sign on behalf of the Bidder. This authorization shall consist of a written confirmation as specified **in the BDS** and shall be attached to the Bid. The name and position held by each person signing the authorization must be typed or printed below the signature. All pages of the Bid where entries or amendments have been made shall be signed or initialed by the person signing the Bid.

21.4 In case the Bidder is a JV, the Bid shall be signed by an authorized representative of the JV on behalf of the JV, and so as to be legally binding on all the members as evidenced by a power of attorney signed by their legally authorized representatives.

21.5 Any interlineations, erasures, or overwriting shall be valid only if they are signed or initialed by the person signing the Bid.

D. SUBMISSION AND OPENING OF BIDS

22. Submission, Sealing and Marking of Bids

22.1 The Bidder shall deliver the Bid in a single, sealed envelope (one (1) envelope process). Within the single envelope the Bidder shall place the following separate, sealed envelopes:

(a) in an envelope marked "ORIGINAL", all documents comprising the Bid, as described in ITB 11; and

(b) in an envelope marked "COPIES", all required copies of the Bid; and,

(c) if alternative Bids are permitted in accordance with ITB 13, and if relevant:

(i) in an envelope marked "ORIGINAL – ALTERNATIVE BID", the alternative Bid; and

(ii) in the envelope marked "COPIES – ALTERNATIVE BID" all required copies of the alternative Bid.

22.2 The inner and outer envelopes shall:

(a) bear the name and address of the Bidder;

(b) be addressed to the Purchaser in accordance with ITB 23.1;

(c) bear the specific identification of this Bidding process indicated in accordance with ITB 1.1; and

(d) Bear a warning not to open before the time and date for Bid opening.

22.3 If all envelopes are not sealed and marked as required, the Purchaser will assume no responsibility for the misplacement or premature opening of the Bid.

23. Deadline for Submission of Bids

23.1 Bids must be received by the Purchaser at the address and no later than the date and time indicated **in the BDS**. When so specified **in the BDS**, Bidders shall have the option of submitting their Bids electronically. Bidders submitting Bids electronically shall follow the electronic Bid submission procedures specified **in the BDS**.

23.2 The Purchaser may, at its discretion, extend this deadline for submission of Bids by amending the bidding documents in accordance with ITB 8, in which case all rights and obligations of the Purchaser and Bidders will thereafter be subject to the deadline as extended.

24. Late Bids

24.1 The Purchaser shall not consider any Bid that arrives after the deadline for submission of Bids, in accordance with ITB 23. Any Bid received by the Purchaser after the deadline for submission of Bids shall be declared late, rejected, and returned unopened to the Bidder.

25. Withdrawal, Substitution, and Modification of Bids

25.1 A Bidder may withdraw, substitute, or modify its Bid after it has been submitted by sending a written notice, duly signed by an authorized representative, and shall include a copy of the authorization in accordance with ITB 21.3, (except that withdrawal notices do not require copies). The corresponding substitution or modification of the Bid must accompany the respective written notice. All notices must be:

(a) prepared and submitted in accordance with ITB 21 and ITB 22 (except that withdrawals notices do not require copies), and in addition, the respective envelopes shall be clearly marked "WITHDRAWAL," "SUBSTITUTION," "MODIFICATION;" and

(b) Received by the Purchaser prior to the deadline prescribed for submission of Bids, in accordance with ITB 23.

25.2 Bids requested to be withdrawn in accordance with ITB 25.1 shall be returned unopened to the Bidders.

25.3 No Bid may be withdrawn, substituted, or modified in the interval between the deadline for submission of Bids and the expiration of the period of Bid validity specified by the Bidder on the Letter of Bid or any extension thereof.

26. Bid Opening

26.1 Except as in the cases specified in ITB 24 and ITB 25.2, the Purchaser shall conduct the Bid opening in public, in the presence of Bidders` designated representatives and anyone who chooses to attend, and at the address, date and time specified **in the BDS**. Any specific electronic Bid opening procedures required if electronic bidding is permitted in accordance with ITB 23.1, shall be as specified **in the BDS**.

26.2 First, envelopes marked "Withdrawal" shall be opened and read out and the envelope with the corresponding Bid shall not be opened, but returned to the Bidder. No Bid withdrawal shall be permitted unless the corresponding withdrawal notice contains a valid authorization to request the withdrawal and is read out at Bid opening.

26.3 Next, envelopes marked "Substitution" shall be opened and read out and exchanged with the corresponding Bid being substituted, and the substituted Bid shall not be opened, but returned to the Bidder. No Bid substitution shall be permitted unless the corresponding substitution notice contains a valid authorization to request the substitution and is read out at Bid opening.

26.4 Envelopes marked "Modification" shall be opened and read out with the corresponding Bid. No Bid modification shall be permitted unless the corresponding modification notice contains a valid authorization to request the modification and is read out at Bid opening. Only Bids that are opened and read out at Bid opening shall be considered further.

26.5 Next, all remaining envelopes shall be opened one at a time, reading out: the name of the Bidder and the Bid Price(s), including any discounts and alternative Bids, and indicating whether there is a modification; the presence or absence of a Bid Security or Bid-Securing Declaration; and any other details as the Purchaser may consider appropriate.

26.6 Only Bids, alternative Bids and discounts that are opened and read out at Bid opening shall be considered further in the evaluation. The Letter of Bid and the Price Schedules are to be initialed by representatives of the Purchaser attending Bid opening in the manner specified **in the BDS**.

26.7 The Purchaser shall neither discuss the merits of any Bid nor reject any Bid (except for late Bids, in accordance with ITB 24.1).

26.8 The Purchaser shall prepare a record of the Bid opening that

shall include, as a minimum:

(a) the name of the Bidder and whether there is a withdrawal, substitution, or modification;

(b) the Bid Price, per lot if applicable, including any discounts;

(c) any alternative Bids; and

(d) The presence or absence of a Bid Security or a Bid-Securing Declaration.

26.9 The Bidders' representatives who are present shall be requested to sign the record. The omission of a Bidder's signature on the record shall not invalidate the contents and effect of the record. A copy of the record shall be distributed to all Bidders.

E. Evaluation and Comparison of Bids

27. Confidentiality

27.1 Information relating to the evaluation of Bids and recommendation of contract award, shall not be disclosed to Bidders or any other persons not officially concerned with the Bidding process until the Notification of Intention to Award the Contract is transmitted to all Bidders in accordance with ITB 42.

27.2 Any effort by a Bidder to influence the Purchaser in the evaluation of the Bids or Contract award decisions may result in the rejection of its Bid.

27.3 Notwithstanding ITB 27.2, from the time of Bid opening to the time of Contract award, if any Bidder wishes to contact the Purchaser on any matter related to the Bidding process, it should do so in writing.

28. Clarification of Bids

28.1 To assist in the examination, evaluation, and comparison of the Bids, and qualification of the Bidders, the Purchaser may, at its discretion, ask any Bidder for a clarification of its Bid. Any clarification submitted by a Bidder that is not in response to a request by the Purchaser shall not be considered. The Purchaser's request for clarification and the response shall be in writing. No change in the prices or substance of the Bid shall be sought, offered, or permitted, except to confirm the correction of arithmetic errors discovered by the Purchaser in the evaluation of the Bids, in accordance with ITB 32.

28.2 If a Bidder does not provide clarifications of its Bid by the date and time set in the Purchaser's request for clarification, its Bid may be rejected.

29. Deviations, Reservations, and Omissions

29.1 During the evaluation of Bids, the following definitions apply:

(a) "Deviation" is a departure from the requirements specified in the bidding document;

(b) "Reservation" is the setting of limiting conditions or withholding from complete acceptance of the requirements specified in the bidding document; and

(c) "Omission" is the failure to submit part or all of the information or documentation required in the bidding document.

30. Determination of Responsiveness

30.1 The Purchaser's determination of a Bid's responsiveness is to be based on the contents of the Bid itself, as defined in ITB 11.

30.2 A substantially responsive Bid is one that meets the requirements of the bidding document without material deviation, reservation, or omission. A material deviation, reservation, or omission is one that;

(a) if accepted, would:

(i) affect in any substantial way the scope, quality, or performance of the Information System specified in the Contract; or

(ii) limit in any substantial way, inconsistent with the bidding document, the Purchaser's rights or the Bidder's obligations under the proposed Contract; or

(b) if rectified, would unfairly affect the competitive position of other Bidders presenting substantially responsive Bids.

30.3 The Purchaser shall examine the technical aspects of the Bid in particular, to confirm that all requirements of Section VII, Purchaser's Requirements have been met without any material deviation, reservation, or omission.

30.4 To be considered for Contract award, Bidders must have submitted Bids:

(a) for which detailed Bid evaluation using the same standards for compliance determination as listed in ITB 29 and ITB 30.3 confirms that the Bids are commercially and technically responsive, and include the hardware, Software, related equipment, products, Materials, and other Goods and Services components of the Information System in substantially the full required quantities for the entire Information System or, if allowed in the BDS ITB 35.8, the individual Subsystem, lot or slice Bid on; and are deemed by the Purchaser as commercially and technically responsive; and

(b) That offer Information Technologies that are proven to perform up to the standards promised in the bid by having successfully passed the performance, benchmark, and/or functionality tests the Purchaser may require, pursuant to ITB 39.3.

31. Nonmaterial Nonconformities

31.1 Provided that a Bid is substantially responsive, the Purchaser may waive any nonconformity in the Bid that does not constitute a material deviation, reservation or omission.

31.2 Provided that a Bid is substantially responsive, the Purchaser may request that the Bidder submit the necessary information or documentation, within a reasonable period of time, to rectify nonmaterial nonconformities in the Bid related to documentation requirements. Requesting information or documentation on such nonconformities shall not be related to any aspect of the price of the Bid. Failure of the Bidder to comply with the request may result in the rejection of its Bid.

31.3 Provided that a Bid is substantially responsive, the Purchaser shall rectify quantifiable nonmaterial nonconformities related to the Bid Price. To this effect, the Bid Price shall be adjusted, for comparison purposes only, to reflect the price of a missing or non-conforming item or component in the manner specified **in the BDS**.

32. Correction of Arithmetical Errors

32.1 Provided that the Bid is substantially responsive, the Purchaser shall correct arithmetical errors on the following basis:

(a) where there are errors between the total of the amounts given under the column for the price breakdown and the amount given under the Total Price, the former shall prevail and the latter will be corrected accordingly;

(b) where there are errors between the total of the amounts of Schedule Nos. 1 to 5 and the amount given in

Schedule No. 6 (Grand Summary), the former shall prevail and the latter will be corrected accordingly; and

(c) if there is a discrepancy between words and figures, the amount in words shall prevail, unless the amount expressed in words is related to an arithmetic error, in which case the amount in figures shall prevail subject to (a) and (b) above.

32.2 A Bidder shall be requested to accept the correction of arithmetical errors. Failure to accept the correction in accordance with ITB 32.1 shall result in the rejection of the Bid.

33. Conversion to Single Currency

33.1 For evaluation and comparison purposes, the currency(ies) of the Bid shall be converted into a single currency as specified **in the BDS**.

34. Margin of Preference

34.1 No margin of domestic preference shall apply.

35. Evaluation of Bids

35.1 The Purchaser shall use the criteria and methodologies listed in this ITB and Section III, Evaluation and Qualification criteria. No other evaluation criteria or methodologies shall be permitted. By applying the criteria and methodologies the Purchaser shall determine the Most Advantageous Bid.

Preliminary Examination

35.2 The Purchaser will examine the bids, to determine whether they have been properly signed, whether required sureties have been furnished, whether any computational errors have been made, whether required sureties have been furnished and are substantially complete (e.g., not missing key parts of the bid or silent on excessively large portions of the Technical Requirements). In the case where a pre-qualification process was undertaken for the Contract(s) for which these bidding documents have been issued, the Purchaser will ensure that each bid is from a pre-qualified bidder and, in the case of a Joint Venture, that partners and structure of the Joint Venture are unchanged from those in the pre-qualification

Technical Evaluation

35.3 The Purchaser will examine the information supplied by the Bidders Pursuant to ITB 11 and ITB 16, and in response to other requirements in the Bidding document, taking into account the following factors:

(a) overall completeness and compliance with the Technical

Requirements; and deviations from the Technical Requirements;

(b) suitability of the Information System offered in relation to the conditions prevailing at the site; and the suitability of the implementation and other services proposed, as described in the Preliminary Project Plan included in the bid;

(c) achievement of specified performance criteria by the Information System;

(d) compliance with the time schedule called for by the Implementation Schedule and any alternative time schedules offered by Bidders, as evidenced by a milestone schedule provided in the Preliminary Project Plan included in the bid;

(e) type, quantity, quality, and long-term availability of maintenance services and of any critical consumable items necessary for the operation of the Information System;

(f) any other relevant technical factors that the Purchaser deems necessary or prudent to take into consideration;

(g) Any proposed deviations in the bid to the contractual and technical provisions stipulated in the bidding documents.

35.4 If specified **in the BDS**, the Purchaser's evaluation of responsive Bids will take into account technical factors, in addition to cost factors. An Evaluated Bid Score (B) will be calculated for each responsive Bid using the formula, specified in Section III, Evaluation and Qualification Criteria, which permits a comprehensive assessment of the Bid cost and the technical merits of each Bid

35.5 Where alternative technical solutions have been allowed in accordance with ITB 13, and offered by the Bidder, the Purchaser will make a similar evaluation of the alternatives. Where alternatives have not been allowed but have been offered, they shall be ignored.

Economic Evaluation

35.6 To evaluate a Bid, the Purchaser shall consider the following:

(a) the Bid price, excluding provisional sums and the provision, if any, for contingencies in the Price Schedules;

(b) price adjustment for correction of arithmetic errors in accordance with ITB 32.1;

(c) price adjustment due to discounts offered in accordance with ITB 26.8;

(d) converting the amount resulting from applying (a) to (c) above, if relevant, to a single currency in accordance with ITB 33; and

(e) price adjustment due to quantifiable nonmaterial nonconformities in accordance with ITB 31.3;

(f) The evaluation factors indicated in Section III, Evaluation and Qualification Criteria.

35.7 If price adjustment is allowed in accordance with ITB 17.9, the estimated effect of the price adjustment provisions of the Conditions of Contract, applied over the period of execution of the Contract, shall not be taken into account in Bid evaluation.

35.8 The Purchaser will evaluate and compare the Bids that have been determined to be substantially responsive, pursuant to ITB 30. The evaluation will be performed assuming either that:

(a) the Contract will be awarded to the Most Advantageous Bid for the entire Information System; or

(b) If specified **in the BDS**, Contracts will be awarded to the Bidders for each individual Subsystem, lot, or slice defined in the Technical Requirements whose Bids result in the Most Advantageous Bid/Bids for the entire System.

In the latter case, discounts that are conditional on the award of more than one Subsystem, lot, or slice may be offered in Bids. Such discounts will be considered in the evaluation of bids as specified **in the BDS**.

36. Comparison of Bids

36.1 The Purchaser shall compare all substantially responsive Bids in accordance with ITB 35.6 to determine the lowest evaluated cost.

37. Abnormally Low Bids

37.1 An Abnormally Low Bid is one where the Bid price in combination with other constituent elements of the Bid appears unreasonably low to the extent that the Bid price raises material concerns as to the capability of the Bidder to perform the Contract for the offered Bid Price.

37.2 In the event of identification of a potentially Abnormally Low Bid, the Purchaser shall seek written clarifications from the

Bidder, including detailed price analyses of its Bid price in relation to the subject matter of the contract, scope, proposed methodology, schedule, allocation of risks and responsibilities and any other requirements of the bidding document.

37.3 After evaluation of the price analyses, in the event that the Purchaser determines that the Bidder has failed to demonstrate its capability to perform the Contract for the offered Bid Price, the Purchaser shall reject the Bid.

38. Unbalanced or Front Loaded Bids

38.1 If the Bid that is evaluated as the lowest evaluated cost is, in the Purchaser's opinion, seriously unbalanced or front loaded the Purchaser may require the Bidder to provide written clarifications. Clarifications may include detailed price analyses to demonstrate the consistency of the Bid prices with the scope of information systems, installations, proposed methodology, schedule and any other requirements of the bidding document.

38.2 After the evaluation of the information and detailed price analyses presented by the Bidder, the Purchaser may:

(a) accept the Bid; or

(b) if appropriate, require that the total amount of the Performance Security be increased, at the expense of the Bidder, to a level not exceeding twenty percent (20%) of the Contract Price; or

(c) reject the Bid.

39. Eligibility and Qualification of the Bidder

39.1 The Purchaser shall determine to its satisfaction whether the Bidder that is selected as having submitted the lowest evaluated and substantially responsive Bid is eligible and meets the qualifying criteria specified in Section III, Evaluation and Qualification Criteria.

39.2 The determination shall be based upon an examination of the documentary evidence of the Bidder's qualifications submitted by the Bidder, pursuant to ITB 15.

39.3 **Unless otherwise specified in the BDS,** the Purchaser will NOT carry out tests at the time of post-qualification, to determine that the performance or functionality of the Information System offered meets those stated in the Technical Requirements. However, if **so specified in the BDS** the Purchaser may carry out such tests **as detailed in the BDS**.

39.4 An affirmative determination shall be a prerequisite for award of the Contract to the Bidder. A negative determination shall

result in disqualification of the Bid, in which event the Purchaser shall proceed to the next lowest evaluated cost or best evaluated Bid, as the case may be, to make a similar determination of that Bidder's qualifications to perform satisfactorily.

39.5 The capabilities of the manufacturers and subcontractors proposed by the Bidder that is determined to have offered the Most Advantageous Bid for identified major items of supply or services will also be evaluated for acceptability in accordance with Section III, Evaluation and Qualification Criteria. Their participation should be confirmed with a letter of intent between the parties, as needed. Should a manufacturer or subcontractor be determined to be unacceptable, the Bid will not be rejected, but the Bidder will be required to substitute an acceptable manufacturer or subcontractor without any change to the Bid price. Prior to signing the Contract, the corresponding Appendix to the Contract Agreement shall be completed, listing the approved manufacturers or subcontractors for each item concerned.

40. Purchaser's Right to Accept Any Bid, and to Reject Any or All Bids

40.1 The Purchaser reserves the right to accept or reject any Bid, and to annul the Bidding process and reject all Bids at any time prior to contract award, without thereby incurring any liability to Bidders. In case of annulment, all Bids submitted and specifically, Bid securities, shall be promptly returned to the Bidders.

41. Standstill Period

41.1 The Contract shall be awarded not earlier than the expiry of the Standstill Period. The duration of the Standstill Period is specified **in the BDS**. Where only one Bid is submitted, the Standstill Period shall not apply.

42. Notice of Intention to Award

42.1 When a Standstill Period applies, it shall commence when the Purchaser has transmitted to each Bidder (that has not already been notified that it has been unsuccessful) Notification of Intention to Award the Contract to the successful Bidder. The Notification of Intention to Award shall contain, at a minimum, the following information:

(a) the name and address of the Bidder submitting the successful Bid;

(b) the Contract price of the successful Bid;

(c) the total combined score of the successful Bid;

(d) the names of all Bidders who submitted Bids, and their

Bid prices as readout and as evaluated prices;

(e) a statement of the reason(s) the Bid (of the unsuccessful Bidder to whom the notice is addressed) was unsuccessful;

(f) the expiry date of the Standstill Period; and

(g) instructions on how to request a debriefing or submit a complaint during the standstill period;

F. AWARD OF CONTRACT

43. Award Criteria

43.1 Subject to ITB 40, the Purchaser shall award the Contract to the successful Bidder. This is the Bidder whose Bid has been determined to be the Most Advantageous Bid. The determination of the Most Advantageous Bid will be made in accordance to one of the two options as defined i**n the BDS**. The methodology options are:

(a) when **rated criteria are used**: The Bidder that meets the qualification criteria and whose Bid:

(i) is substantially responsive; and

(ii) is the best evaluated Bid (i.e. the Bid with the highest combined technical/quality/price score); or

(b) when **rated criteria are not used**: The Bidder that meets the qualification criteria and whose Bid has been determined to be:

(i) substantially responsive to the bidding document; and

(ii) The lowest evaluated cost.

44. Purchaser's Right to Vary Quantities at Time of Award

44.1 The Purchaser reserves the right at the time of Contract award to increase or decrease, by the percentage(s) for items as indicated **in the BDS.**

45. Notification of Award

45.1 Prior to the expiration of the Bid Validity Period and upon expiry of the Standstill Period, specified in PDS ITB 41.1 or any extension thereof, or upon satisfactorily addressing a complaint that has been filed within the Standstill Period, the Purchaser shall notify the successful Bidder, in writing, that its Bid has been accepted. The notification letter (hereinafter and in the Conditions of Contract and Contract Forms called the "Letter of Acceptance") shall specify the sum that the Purchaser will pay the Supplier in consideration of the execution of the Contract (hereinafter and in the Conditions of Contract and Contract Forms called "the Contract Price").

45.2 At the same time, the Purchaser shall publish the Contract Award Notice which shall contain, at a minimum, the following information:

(a) name and address of the Purchaser;

(b) name and reference number of the contract being awarded, and the selection method used;

(c) names of all Bidders that submitted Bids, and their Bid prices as read out at Bid opening, and as evaluated;

(d) name of Bidders whose Bids were rejected and the reasons for their rejection; and

(e) The name of the successful Bidder, the final total contract price, the contract duration and a summary of its scope.

44.3 The Contract Award Notice shall be published on the Purchaser's website with free access if available, or in at least one newspaper of national circulation in the Purchaser's Country, or in the official gazette. The Purchaser shall also publish the Contract Award Notice in UNDB online.

44.4 Until a formal contract is prepared and executed, the Notification of Award shall constitute a binding Contract.

45. Debriefing by the Purchaser

45.1 On receipt of the Borrower's Notification of Intention to Award referred to in ITB 42, an unsuccessful Bidder has three (3) Business Days to make a written request to the Purchaser for a debriefing. The Purchaser shall provide a debriefing to all unsuccessful Bidders whose request is received within this deadline.

45.2 Where a request for debriefing is received within the deadline, the Purchaser shall provide a debriefing within five (5) Business Days, unless the Purchaser decides, for justifiable reasons, to provide the debriefing outside this timeframe. In that case, the standstill period shall automatically be extended until

five (5) Business Days after such debriefing is provided. If more than one debriefing is so delayed, the standstill period shall not end earlier than five (5) Business Days after the last debriefing takes place. The Purchaser shall promptly inform, by the quickest means available, all Bidders of the extended standstill period.

45.3 Where a request for debriefing is received by the Purchaser later than the three (3)-Business Day deadline, the Purchaser should provide the debriefing as soon as practicable, and normally no later than fifteen (15) Business Days from the date of publication of Public Notice of Award of contract. Requests for debriefing received outside the three (3)-day deadline shall not lead to extension of the standstill period.

45.4 Debriefings of unsuccessful Bidders may be done in writing or verbally. The Bidder shall bear own costs of attending such a debriefing meeting.

46. Signing of Contract

46.1 Promptly upon Notification of Award, the Purchaser shall send the successful Bidder the Contract Agreement.

46.2 Within twenty-eight (28) days of receipt of the Contract Agreement, the successful Bidder shall sign, date, and return it to the Purchaser.

46.3 Notwithstanding ITB 46.2 above, in case signing of the Contract Agreement is prevented by any export restrictions attributable to the Purchaser, to the country of the Purchaser, or to the use of the Information System to be supplied, where such export restrictions arise from trade regulations from a country supplying those Information System, the Bidder shall not be bound by its Bid, always provided, however, that the Bidder can demonstrate to the satisfaction of the Purchaser and of the Bank that signing of the Contract Agreement has not been prevented by any lack of diligence on the part of the Bidder in completing any formalities, including applying for permits, authorizations and licenses necessary for the export of the Information System under the terms of the Contract.

47. Performance Security

47.1 Within twenty-eight (28) days of the receipt of the Letter of Acceptance from the Purchaser, the successful Bidder shall furnish the performance security in accordance with the General Conditions, subject to ITB 38.2 (b), using for that purpose the Performance Security Form included in Section X, Contract Forms, or another form acceptable to the Purchaser. If the Performance Security furnished by the successful Bidder is in the form of a bond, it shall be issued by a bonding or insurance company that has been determined by the successful Bidder to be acceptable to the Purchaser. A foreign institution providing a Performance Security shall have a correspondent financial institution located in the Purchaser's Country.

47.2 Failure of the successful Bidder to submit the above-mentioned Performance Security or sign the Contract shall constitute sufficient grounds for the annulment of the award and forfeiture of the Bid Security. In that event the Purchaser may award the Contract to the Bidder offering the next Most Advantageous Bid.

48. Adjudicator

48.1 Unless **the BDS** states otherwise, the Purchaser proposes that the person named **in the BDS** be appointed as Adjudicator under the Contract to assume the role of informal Contract dispute mediator, as described in GCC Clause 43.1. In this case, a résumé of the named person is attached to the BDS. The proposed hourly fee for the Adjudicator is specified in the BDS. The expenses that would be considered reimbursable to the Adjudicator are also specified **in the BDS**. If a Bidder does not accept the Adjudicator proposed by the Purchaser, it should state its non-acceptance in its Bid Form and make a counterproposal of an Adjudicator and an hourly fee, attaching a résumé of the alternative. If the successful Bidder and the Adjudicator nominated **in the BDS** happen to be from the same country, and this is not the country of the Purchaser too, the Purchaser reserves the right to cancel the Adjudicator nominated **in the BDS** and propose a new one. If by the day the Contract is signed, the Purchaser and the successful Bidder have not agreed on the appointment of the Adjudicator, the Adjudicator shall be appointed, at the request of either party, by the Appointing Authority specified in the SCC clause relating to GCC Clause 43.1.4, or if no Appointing Authority is specified there, the Contract will be implemented without an Adjudicator.

SECTION II - BID DATA SHEET (BDS)

The following specific data for the Information System to be procured shall complement, supplement, or amend the provisions in the Instructions to Bidders (ITB). Whenever there is a conflict, the provisions herein shall prevail over those in ITB.

ITB Reference	A. General
ITB 1.1	The reference number of the Request for Bids is : AF-G5 The Purchaser is: Bangladesh Computer Council (BCC) represented by Project Director, Leveraging ICT for Growth, Employment & Governance Project. The name of the RFB is: Supply, Installation and Commissioning of Hardware & Software for Establishment of Cyber Defense Training Center at BCC. The number and identification of lots (contracts) comprising this RFB is: One.
ITB 1.3 (a)	**Not Applicable.**
ITB 2.1	The Borrower is: **The People's Republic of Bangladesh.** Loan or Financing Agreement amount: **US$ 39 million *(Additional Financing)*** The name of the Project is: **Leveraging ICT for Growth, Employment & Governance Project.**
ITB 4.1	Maximum number of members in the JV shall be: **it is preferable to limit maximum three members in the Joint venture.**
ITB 4.5	A list of debarred firms and individuals is available on the Bank's external website: http://www.worldbank.org/debarr.
	B. Bidding Document
ITB 7.1	For **Clarification of Bid purposes** only, the Purchaser's address is: Attention: *Md. Rezaul Karim ndc, Project Director* Address: 2nd Floor , Bangladesh Computer Council (BCC), ICT Tower (Old BCC Bhaban), Plot # E-14/X, Agargaon, Sher-e-Bangla Nagar, Dhaka – 1207, Bangladesh Telephone:+88-02-8181381 Facsimile: +88-02-8181383 E-mail: pd.lict@bcc.net.bd Requests for clarification should be received by the Purchaser no later than: **21**

	days from the date of publication of the Request for Bid.
ITB 7.1	Web page: **www.bcc.gov.bd**
ITB 7.4	A Pre-Bid meeting ***shall*** take place at the following date, time and place: Date: 11 September 2017 Time: 11.00 am BST (Local Time) Place: Leveraging ICT for Growth, Employment and Governance Project, Bangladesh Computer Council (BCC), Agargaon, Dhaka-1207, Bangladesh A site visit conducted by the Purchaser ***shall not be*** organized.
C. Preparation of Bids	
ITB 10.1	The language of the Bid is: **English.** All correspondence exchange shall be in **English** language. Language for translation of supporting documents and printed literature is **English.**
ITB 11.1 (k)	The Bidder shall submit with its Bid the following additional documents: A. Certificate of Incorporation and Trade License; B. Work Order and Work Completion Certificate mentioning contract value, time, work summary, purchaser's detailed contact information etc.; C. Declaration confirming that all hardware, software, tool, systems would be in the name of purchaser "Bangladesh Computer Council" during sourcing and supply. Bidder must follow the authorized OEM's channel for the end purchaser's territory to ensure originality of the supplied products and future support services and warranty/replacement; D. Audited Balance Sheet and Income Statement; E. Bank Certificate mentioning undrawn balance in case of credit line which shall be made available to the Bidder; F. Details of work experience; and G. CVs of Team members.
ITB 13.1	Alternative Bids are not permitted.
ITB 13.2	Alternatives to the Time Schedule are not permitted.
ITB 13.4	Alternative technical solutions shall be permitted for the following parts of the Information System: **Not applicable.**
ITB 15.2	Prequalification **has not** been undertaken.

ITB 16.2 (a)	In addition to the topics described in ITB Clause 16.2 (a), the Preliminary Project Plan must address the following topics : ***(a) Project Organization and Management Sub-Plan, including management authorities, responsibilities, and contacts, as well as task, time and resource-bound schedules (in GANTT format);*** ***(b) Implementation Sub-Plan;*** ***(c) Training Sub-Plan;*** ***(d) Testing and Quality Assurance Sub-Plan;*** ***(e) Warranty Defect Repair and Technical Support Service Sub-Plan***
ITB 16.3	In the interest of effective integration, cost-effective technical support, and reduced re-training and staffing costs, Bidders are required to offer specific brand names and models for the following limited number of specific items: **None**.
ITB 17.2	The Bidder *must not* bid Recurrent Cost Items.
ITB 17.2	The Bidder *must not* bid for contracts of Recurrent Cost Items not included in the main Contract.
ITB 17.5	The Incoterms edition is Inco terms 2010 — ICC Official Rules for the Interpretation of Trade Terms" published by the International Chamber of Commerce, 38 Courts Albert 1er, 75008 Paris, France
ITB 17.5 (a)	Named place of destination is: Leveraging ICT for Growth, Employment & Governance Project Bangladesh Computer Council (BCC), 2nd Floor, ICT Tower (Old BCC Bhaban), Plot # E-14/X, Agargaon, Sher-e-Bangla Nagar, Dhaka – 1207, Bangladesh.
ITB 17.6	Named place of final destination (or Project site) is: Leveraging ICT for Growth, Employment & Governance Project Bangladesh Computer Council (BCC), 2nd Floor, ICT Tower (Old BCC Bhaban), Plot # E-14/X, Agargaon, Sher-e-Bangla Nagar, Dhaka – 1207, Bangladesh.
ITB 17.8.1	In addition to ITB 17.8 following ITB 17.8.1 clause to be added: **Beyond the Contract Price, the following *expenses incidental to the performance of Services and incurred* by the Supplier, which the Purchaser will reimburse at cost against receipts:** (a) **Customs Duty and any other taxes payable at the port(s) as per the rules of the Government of Bangladesh.** (b) **C&F costs.**

ITB 17.9	The prices quoted by the Bidder ***shall not*** be subject to adjustment during the performance of the Contract.
ITB 18.1	The Bidder ***is*** required to quote in the currency of the Purchaser's Country the portion of the Bid price that corresponds to expenditures incurred in that currency.
ITB 19.1	The Bid validity period shall be **one hundred fifty (150*)*** days after the deadline for bid submission, as specified below in reference to ITB Clause 23.1.
ITB 19.3 (a)	The Bid price shall be adjusted by the following factor(s): **Not Applicable.**
ITB 20.1	A *Bid Security* ***shall be*** required. A Bid-Securing Declaration ***shall not be*** required. The amount and currency of the Bid Security shall be United States Dollar (US$) 25,000 (US$ Twenty Five Thousand only) or BDT 2,000,000 (BDT Two Million Only) or an equivalent amount in a freely convertible currency. The Bid Security shall be valid for twenty-eight (28) days beyond the original validity period of the Bid, or beyond any period of extension if requested under ITB 19.2. Accordingly, a bid with a **Bid Security** that expires before t**he required date of the expiration of the Bid Security (i.e. twenty-eight (28) days after the end of the bid validity period)** shall be rejected as non-responsive.
ITB 20.3 (d)	The ITB clause 20.3 will be modified as follows: a) **Bid Security shall be in the form of an unconditional guarantee issued from a reputable Bank and an eligible country (in case the Bank is located outside the Purchaser's country, it shall have a correspondent Bank in the Employer's country to make it enforceable).** b) **Bid security shall be submitted using the Bid Security Form included in Section IV.**
ITB 20.10	Not Applicable.
ITB 21.1	Required number of bid copies: Original plus two (2) copies. **In addition, one soft copy of the bid in MS-Word document has to be submitted in CD/DVD in a sealed envelope. In case of any discrepancy in between the paper based bid and the soft copy of the bid, the paper based bid shall prevail.**

ITB 21.3	The written confirmation of authorization to sign on behalf of the Bidder shall consist of: a. The name and description of the documentation required to demonstrate the authority of the signatory to sign the Bid such as a Power of Attorney; and b. In the case of Bids submitted by an existing or intended JV an undertaking signed by all parties (i) stating that all parties shall be jointly and severally liable, and (ii) nominating a Representative who shall have the authority to conduct all business for and on behalf of any and all the parties of the JV during the bidding process and, in the event the JV is awarded the Contract, during contract execution.
D. Submission and Opening of Bids	
ITB 23.1	For **Bid submission purposes** only, the Purchaser's address is : ***[This address may be the same as or different from that specified under provision ITB 7.1 for clarifications]*** Place: Office of the Project Director Leveraging ICT for Growth, Employment and Governance Project Bangladesh Computer Council (BCC) ICT Tower (2nd Floor), Agargaon, Dhaka-1207, Bangladesh. **The deadline for Bid submission is:** Date: 09 October 2017 Time: 15:00 Hours BST (GMT+6 hours)
ITB 23.1	Bidders ***shall not*** have the option of submitting their Bids electronically.
ITB 26.1	The Bid opening shall take place at: Place: Office of the Project Director Leveraging ICT for Growth, Employment and Governance Project Bangladesh Computer Council (BCC) ICT Tower (2nd Floor), Agargaon, Dhaka-1207, Bangladesh. Date: 09 October 2017 Time: 15:30 Hours BST (GMT+6 hours)
ITB 26.1	The electronic Bid opening procedures shall be: **Not Applicable.**
ITB 26.6	The Letter of Bid and Price Schedules shall be initialed by **3 (three)** representatives of the Purchaser conducting Bid opening. **Each Bid shall be initialed by all representatives and shall be numbered, any modification to the unit or total price shall be initialed by the Representative of the Purchaser, etc.**

E. Evaluation, and Comparison of Bids	
ITB 31.3	The adjustment shall be based on the ***highest*** price of the item or component as quoted in other substantially responsive Bids. If the price of the item or component cannot be derived from the price of other substantially responsive Bids, the Purchaser shall use its best estimate. If the missing Goods and Services are a scored technical feature, the relevant score will be set at zero.
ITB 33.1	The currency (ies) of the Bid shall be converted into a single currency as follows: Bangladesh Taka (BDT). The currency that shall be used for Bid evaluation and comparison purposes to convert all Bid prices expressed in various currencies into a single currency is: Bangladesh Taka (BDT) The source of exchange rate shall be: Bangladesh Bank, Dhaka, and the latest selling rate available on the date mentioned below in the web site http://www.bangladesh-bank.org/ shall be used. The date for the exchange rate shall be: **Fourteen (14)** days prior to the date of bid submission. In case that no exchange rates are available on this date from the source indicated above, the latest available exchange rates from the same source prior to this date will be used.
ITB 35.4	The Purchaser's evaluation of responsive Bids ***will not take*** into account technical factors, in addition to cost factors as specified in Section III, Bid Evaluation and Qualification Criteria.
ITB 35.4	Interest Rate (I) for net present value calculations of recurrent costs is **not required.** The bid evaluation **will not** take into account technical factors in addition to cost factors.
ITB 35.8	Bids for Subsystems, lots, or slices of the overall Information System **will not be** accepted. Discount that are conditional on the award of more than one Subsystem, lot, or slice may be offered in Bids and such discounts ***shall not*** be considered in the price evaluation.
ITB 39.3	**Not Applicable.**
ITB 41	The Standstill Period is **ten (10)** Business Days from the date the Purchaser has transmitted to all Proposers that submitted Proposals, the Notification of its Intention to Award the Contract to the successful Proposer.

ITB 43	The award will be made on the basis of *"**not rated" criteria*** pursuant to ITB 35.7, if applicable, in accordance with Section III, Evaluation and Qualification Criteria.
ITB 44	The maximum percentage by which quantities may be increased is: ***20%*** The maximum percentage by which quantities may be decreased is: ***20%*** The items for which the Purchaser may increase of decrease the quantities are the following. All Items
ITB 48	The proposed Adjudicator is: An Adjudicator shall be agreed by the Purchaser and the Bidder before the finalization of the Contract. The proposed hourly fee and the expenses that would be considered reimbursable to the Adjudicator shall also be agreed by the Purchaser and the Supplier before finalization of the Contract.

SECTION III - EVALUATION AND QUALIFICATION CRITERIA (WITHOUT PREQUALIFICATION)

This Section contains all the criteria that the Purchaser shall use to evaluate Bids and qualify Bidders. No other factors, methods or criteria shall be used. The Bidder shall provide all the information requested in the forms included in Section IV, Bidding Forms.

1. Evaluation

The Purchaser will evaluate and compare the Bids that have been determined to be substantially responsive, pursuant to ITB 30. **Not Applicable.**

If indicated by the BDS, the Purchaser's evaluation of responsive Bids will take into account technical factors, in addition to cost factors.

In such a case, an Evaluated Bid Score (B) will be calculated for each responsive Bid using the following formula, which permits a comprehensive assessment of the Bid price and the technical merits of each Bid:

$$B \equiv \frac{C_{low}}{C} X + \frac{T}{T_{high}}(1 - X)$$

where

C = Evaluated Bid Price

C_{low} = the lowest of all Evaluated Bid Prices among responsive Bids

T = the total Technical Score awarded to the Bid

T_{high} = the Technical Score achieved by the Bid that was scored best among all responsive Bids

X = weight for the Price as specified in the BDS

The Bid with the best evaluated Bid Score (B) among responsive Bids shall be the Most Advantageous Bid provided the Bidder was prequalified and/or it was found to be qualified to perform the Contract in accordance with ITB 39.

If, in addition to the cost factors, the Purchaser has chosen to give weight to important technical factors (i.e., the price weight, X, is less than 1 in the evaluation), that cannot be reduced to life-cycle costs or pass/fail criteria, the Total Technical Points assigned to each Bid in the Evaluated Bid Formula will be determined by adding and weighting the scores assigned by an evaluation committee to technical features of the Bid in accordance with the criteria set forth below.

(a) The technical features to be evaluated are generally defined below and specifically identified **in the BDS**:

(i) Performance, capacity, or functionality features that either exceed levels specified as mandatory in the Technical Requirements; and/or influence the life-cycle cost and effectiveness of the Information System.

(ii) Usability features, such as ease of use, ease of administration, or ease of expansion, which influence the life-cycle cost and effectiveness of the Information System.

(iii) The quality of the Bidder's Preliminary Project Plan as evidenced by the thoroughness, reasonableness, and responsiveness of: (a) the task and resource

schedules, both general and specific, and (b) the proposed arrangements for management and coordination, training, quality assurance, technical support, logistics, problem resolution, and transfer of knowledge, and other such activities as specified by the Purchaser in Section VII, Technical Requirements or proposed by the Bidder based on the Bidder's experience.

(iv) Any sustainable procurement requirement if specified in Section VII- Requirements of the Information System.

(b) Feature scores will be grouped into a small number of evaluation categories, generally defined below and specifically identified in the BDS, namely:

(i) The technical features that reflect how well the Information System meets the Purchaser's Business Requirements (including quality assurance and risk-containment measures associated with the implementation of the Information System).

(ii) The technical features that reflect how well the Information System meets the System's Functional Performance Standards.

(iii) The technical features that reflect how well the Information System meets the General Technical Requirements for hardware, network and communications, Software, and Services.

(c) As specified **in the BDS**, each category will be given a weight and within each category each feature may also be given a weight.

(d) During the evaluation process, the evaluation committee will assign each desirable/preferred feature a whole number score from 0 to 4, where 0 means that the feature is absent, and 1 to 4 either represent predefined values for desirable features amenable to an objective way of rating (as is the case for, e.g., extra memory, or extra mass storage capacity, etc., if these extras would be conducive for the utility of the system), or if the feature represents a desirable functionality (e.g., of a software package) or a quality improving the prospects for a successful implementation (such as the strengths of the proposed project staff, the methodology, the elaboration of the project plan, etc., in the bid), the scoring will be 1 for the feature being present but showing deficiencies; 2 for meeting the requirements; 3 for marginally exceeding the requirements; and 4 for significantly exceeding the requirements.

(e) The score for each feature (i) within a category (j) will be combined with the scores of features in the same category as a weighted sum to form the Category Technical Score using the following formula:

$$S_j \equiv \sum_{i=1}^{k} t_{ji} * w_{ji}$$

where:

t_{ji} = the technical score for feature "i" in category "j"

w_{ji} = the weight of feature "i" in category "j"

k = the number of scored features in category "j"

and $\sum_{i=1}^{k} w_{ji} = 1$

(f) The Category Technical Scores will be combined in a weighted sum to form the total Technical Bid Score using the following formula:

$$T \equiv \sum_{j=1}^{n} S_j * W_j$$

where:

S_j = the Category Technical Score of category "j"

W_j = the weight of category "j" as specified in the BDS

n = the number of categories

and $\sum_{j=1}^{n} W_j = 1$

1.1 Technical Evaluation (ITB 35.3 to ITB 35.4) – Not Applicable.

In addition to the criteria listed in ITB 35.3 (a) and (e), the following factors shall apply:

1.2 Economic Evaluation- Not Applicable.

The following factors and methods will apply:

(a) Time Schedule:

Time to complete the Information System from the effective date specified in Article 3 of the Contract Agreement for determining time for completion of pre-commissioning activities is: _____. No credit will be given for earlier completion.

or

Time to complete the Information System from the effective date specified in Article 3 of the Contract Agreement for determining time for completion of pre-commissioning activities shall be between _____ minimum and _____ maximum. The adjustment rate in the event of completion beyond the minimum period shall be _____ for each week of delay from that minimum period. No credit will be given for completion earlier than the minimum designated period. Bids offering a completion date beyond the maximum designated period shall be rejected.

(b) Recurrent Costs

Since the operation and maintenance of the system being procured form a major part of the implementation, the resulting recurrent costs will be evaluated according to the principles given hereafter, including the cost of recurrent cost items for the initial period of operation stated below, based on prices furnished by each Bidder in Price Schedule Nos. 3.3 and 3.5.

Recurrent cost items for post- warranty service period if subject to evaluation shall be included in the main contract or a separate contract signed together with the main contract.

Such costs shall be added to the Bid price for evaluation.

Option 1: The recurrent costs factors for calculation of the implementation schedule are: Recurrent costs are not considered under the scope of this bid.

The Recurrent Costs (R) are reduced to net present value and determined using the following formula:

$$R \equiv \sum_{x=1}^{N+M} \frac{R_x}{(1+I)^x}$$

Where

N = number of years of the Warranty Period, defined in SCC Clause 29.4

M = number of years of the Post-Warranty Services Period, as defined in SCC Clause 1.1.(e) (xii)

x = an index number 1, 2, 3, ... N + M representing each year of the combined Warranty Service and Post-Warranty Service Periods.

R_x = total Recurrent Costs for year "x," as recorded in the Recurrent Cost Sub-Table.

I = discount rate to be used for the Net Present Value calculation, as **specified in the PDS 35.3.**

Or Option 2: Reference to the methodology specified in the Specification or elsewhere in the bidding document.

(c) Specific additional criteria

The relevant evaluation method, if any, shall be as follows:

1.3 Technical alternatives - Not Applicable.

If invited in accordance with ITB 13.4, will be evaluated as follows:

……
……

2. Qualification

Factor	2.1 ELIGIBILITY					
Sub-Factor	Criteria					Documentation Required
	Requirement	Bidder				
		Single Entity	Joint Venture (existing or intended)			
			All members combined	Each member	At least one member	
2.1.1 Nationality	Nationality in accordance with ITB 4.4.	Must meet requirement	N/A	Must meet requirement	N / A	Form ELI –2.1.1 and 2.1.2, with attachments
2.1.2 Conflict of Interest	No- conflicts of interests as described in ITB 4.2.	Must meet requirement	N/A	Must meet requirement	N / A	Letter of Bid
2.1.3 Bank Ineligibility	Not having been declared ineligible by the Bank as described in ITB 4.5.	Must meet requirement	N/A	Must meet requirement	N / A	Letter of Bid
2.1.4 State owned Entity of the Borrower country	Compliance with conditions of ITB 4.6	Must meet requirement	N/A	Must meet requirement	N / A	Form ELI –2.1.1 and 2.1.2, with attachments
2.1.5 United Nations resolution or Borrower's country law	Not having been excluded as a result of prohibition in the Borrower's country laws or official regulations against commercial relations with the Bidder's country, or by an act of compliance with UN Security Council resolution, both in accordance with ITB 4.8	Must meet requirement	N/A	Must meet requirement	N / A	Letter of Bid

Factor	2.2 HISTORICAL CONTRACT NON-PERFORMANCE					
Sub-Factor	Criteria					Documentation Required
	Requirement	Bidder				
		Single Entity	Joint Venture (existing or intended)			
			All members combined	Each member	At least one member	
2.2.1 History of non-performing contracts	Non-performance of a contract[1] did not occur as a result of Bidder's default since 1st January *2013*.	Must meet requirement by itself or as member to past or existing JV	N / A	Must meet requirement[2]	N / A	Form CON - 2
2.2.2 Suspension	Suspension Based on Execution of Bid Securing Declaration by the Employer or withdrawal of the Bid within Bid validity	Not under suspension based on execution of a Bid Securing Declaration pursuant to ITB 4.7 or withdrawal of the Bid pursuant ITB 20.10	N / A	Must meet requirement	N / A	Letter of Bid

[1] Nonperformance, as decided by the Purchaser, shall include all contracts where (a) nonperformance was not challenged by the contractor, including through referral to the dispute resolution mechanism under the respective contract, and (b) contracts that were so challenged but fully settled against the contractor. Nonperformance shall not include contracts where Purchaser decision was overruled by the dispute resolution mechanism. Nonperformance must be based on all information on fully settled disputes or litigation, i.e. dispute or litigation that has been resolved in accordance with the dispute resolution mechanism under the respective contract and where all appeal instances available to the applicant have been exhausted.

[2] This requirement also applies to contracts executed by the Applicant as JV member.

Factor	2.2 HISTORICAL CONTRACT NON-PERFORMANCE					
Sub-Factor	Criteria					Documentation Required
	Requirement	Bidder				
		Single Entity	Joint Venture (existing or intended)			
			All members combined	Each member	At least one member	
2.2.3 Pending Litigation	Bidder's financial position and prospective long term profitability still sound according to criteria established in 2.3.1 below and assuming that all pending litigation will be resolved against the Bidder.	Must meet requirement by itself or as member to past or existing JV.	N / A	Must meet requirement	N / A	Form CON – 2

Factor	2.3 FINANCIAL SITUATION					
Sub-Factor	Criteria					Documentation Required
	Requirement	Bidder				
		Single Entity	Joint Venture (existing or intended)			
			All members combined	Each member	At least one member	
2.3.1 Historical Financial Performance	Submission of audited balance sheets or if not required by the law of the Bidder's country, other financial statements acceptable to the Purchaser, for the last three [03] years to demonstrate the current soundness of the Bidders financial position and its prospective long term profitability.	Must meet requirement	N / A	Must meet requirement	N / A	Form FIN – 2.3.1 with attachments
2.3.2 Average Annual Turnover	Minimum average annual turnover of US$ 1.5 million or equivalent amount, calculated as total certified payments received for contracts in progress or completed, within the last three (03) years	Must meet requirement	100%	Must meet 25% of the requirement	Must meet 40% of the requirement	Form FIN –2.3.2

Factor	2.3 FINANCIAL SITUATION					
Sub-Factor	Criteria					Documentation Required
	Requirement	Bidder				
		Single Entity	Joint Venture (existing or intended)			
			All members combined	Each member	At least one member	
2.3.3 Financial Resources	The Bidder must demonstrate access to, or availability of, financial resources such as liquid assets, unencumbered real assets, lines of credit, and other financial means, other than any contractual advance payments to meet the following cash-flow requirement: minimum US$ 1 million or equivalent amount.	Must meet requirement	100%	Must meet 25% of the requirement	Must meet 40% of the requirement	Form FIN –2.3.3

Factor	2.4 EXPERIENCE					
Sub-Factor	Criteria					Documentation Required
	Requirement	Bidder				
		Single Entity	Joint Venture (existing or intended)			
			All members combined	Each member	At least one member	
2.4.1 General Experience	Experience under Information System contracts in the role of prime supplier, management contractor, JV member, or subcontractor for at least the last three [03] years prior to the applications submission deadline.	Must meet requirement	N / A	Must meet requirement	N / A	Form EXP-2.4.1
2.4.2 Specific Experience	The Bidder/SI/OEM must have experience of Supply, Installation, Commissioning and Integration of Cyber Attack Simulation Lab or equivalent, from which at least 3 should be functional and in operation for minimum of 12 months	Must meet requirement	N / A	N/A	Must meet requirement	Form EXP-2.4.2
2.4.3 Specific Experience	Participation as a prime supplier, in at least one (01) contract within the last five (05) years 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. The contract will be treated as similar, which includes setting up or establishment of Cyber Attack Simulation, items of those described in Section VII, Purchaser's Requirements.	Must meet requirement	N/A	N / A	Must meet requirement	Form EXP 2.4.2

2.5

2.5.1 Personnel

The Bidder must demonstrate that it will have the personnel for the key positions that meet the following requirements:

1. The Bidder/SI/OEM must have its own Cyber Security Research Team with at least 50 engineers on-board.

2. The Bidder/SI/OEM proposed technical team must have least two (2) of the following certifications:
   - Certified Information Systems Security Professional (CISSP), granted by the International Information System Security Certification Consortium (ISC)².
   - GIAC Certified Intrusion Analyst
   - Cisco Certified Internetwork Expert (Security)
   - EC Council Certified Security Analyst
   - ISACA Certified CSX Practitioner

3. The Bidder/SI/OEM must provide Technical team's qualification details mentioning
   a. the technical expertise area
   b. certifications
   c. experience

Important Note: The Bidder/SI/OEM must provide documentary evidence supporting their citations regarding the all of the above qualification criteria. The Bidder/SI/OEM shall provide details of the proposed personnel and their experience records in the relevant Forms included in Section IV, Bidding Forms.

2.5.2 Subcontractors /Vendors/ Original Equipment Manufacturers (OEM) /System Integrators

Subcontractors/vendors/manufacturers for the following major items of supply or services must meet the following minimum criteria, herein listed for that item:

For all items under this bid, the Bidder/SI/OEM must comply with technical specifications and requirements mentioned in this Request for Bid (RFP). Failure to comply with this requirement will result in rejection of the subcontractor/vendor.

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. The Bidder is responsible for ensuring that the manufacturer or producer complies with the requirements of ITB 4 and 5 and meets the minimum criteria listed above for that item.

The winning bidder must arrange Proof of Concept (POC) at Original Equipment Manufacturer (OEM) facility for at least three persons.

SECTION IV - BIDDING FORMS

Table of Forms

Letter of Bid

INSTRUCTIONS TO BIDDERS: DELETE THIS BOX ONCE YOU HAVE COMPLETED THE DOCUMENT

The Bidder must prepare this Letter of Bid on stationery with its letterhead clearly showing the Bidder's complete name and business address.

Note: All italicized text is to help Bidders in preparing this form.

Date of this Bid submission: [*insert date (as day, month and year) of Bid submission*]

RFB No.: [*insert number of RFB process*]

Alternative No.: [*insert identification No if this is a Bid for an alternative*]

To: **[*insert complete name of Purchaser]***

(a) **No reservations:** We have examined and have no reservations to the bidding document, including Addenda issued in accordance with Instructions to Bidders (ITB 8);

(b) **Eligibility**: We meet the eligibility requirements and have no conflict of interest in accordance with ITB 4;

(c) **Bid-Securing Declaration:** We have not been suspended nor declared ineligible by the Purchaser based on execution of a Bid-Securing Declaration in the Purchaser's Country in accordance with ITB 4.7;

(d) **Conformity:** We offer to provide design, supply and installation services in conformity with the bidding document of the following: [*insert a brief description of the IS Design, Supply and Installation Services*];

(e) Bid Price: The total price of our Bid, excluding any discounts offered in item (f) below is: *[Insert one of the options below as appropriate]*

[Option 1, in case of one lot:] Total price is: [*insert the total price of the Bid in words and figures, indicating the various amounts and the respective currencies*];

Or

[Option 2, in case of multiple lots:] (a) Total price of each lot [*insert the total price of each lot in words and figures, indicating the various amounts and the respective currencies*]; and (b) Total price of all lots (sum of all lots) [*insert the total price of all lots in words and figures, indicating the various amounts and the respective currencies*];

(f) **Discounts:** The discounts offered and the methodology for their application are:

(i) The discounts offered are: [*Specify in detail each discount offered.*]

(ii) The exact method of calculations to determine the net price after application of discounts is shown below: [*Specify in detail the method that shall be used to apply the discounts*];

(g) **Bid Validity Period:** Our Bid shall be valid for the period specified in BDS ITB 19.1 (as amended if applicable) from the date fixed for the Bid submission deadline (specified in BDS ITB 23.1 (as amended if applicable), and it shall remain binding upon us and may be accepted at any time before the expiration of that period;

(h) **Performance Security:** If our Bid is accepted, we commit to obtain a Performance Security in accordance with the bidding document;

(i) **One Bid Per Bidder:** We are not submitting any other Bid(s) as an individual Bidder, and we are not participating in any other Bid(s) as a Joint Venture member, and meet the requirements of ITB 4.3, other than alternative Bids submitted in accordance with ITB 13;

(j) **Suspension and Debarment**: We, along with any of our subcontractors, suppliers, consultants, manufacturers, or service providers for any part of the contract, are not subject to, and not controlled by any entity or individual that is subject to, a temporary suspension or a debarment imposed by the World Bank Group or a debarment imposed by the World Bank Group in accordance with the Agreement for Mutual Enforcement of Debarment Decisions between the World Bank and other development banks. Further, we are not ineligible under the Purchaser's Country laws or official regulations or pursuant to a decision of the United Nations Security Council;

(k) **State-owned enterprise or institution**: [*select the appropriate option and delete the other*] [*We are not a state-owned enterprise or institution*] / [*We are a state-owned enterprise or institution but meet the requirements of ITB 4.6*];

(l) **Commissions, gratuities and fees**: We have paid, or will pay the following commissions, gratuities, or fees with respect to the Bidding process or execution of the Contract: *[insert complete name of each Recipient, its full address, the reason for which each commission or gratuity was paid and the amount and currency of each such commission or gratuity]*

Name of Recipient	Address	Reason	Amount

(If none has been paid or is to be paid, indicate "none.")

(m) **Binding Contract**: We understand that this Bid, together with your written acceptance thereof included in your Letter of Acceptance, shall constitute a binding contract between us, until a formal contract is prepared and executed;

(n) **Not Bound to Accept:** We understand that you are not bound to accept the lowest evaluated cost Bid, the Most Advantageous Bid or any other Bid that you may receive; and

(o) **Fraud and Corruption:** We hereby certify that we have taken steps to ensure that no person acting for us or on our behalf engages in any type of Fraud and Corruption.

Name of the Bidder: *[*insert complete name of person signing the Bid*]

Name of the person duly authorized to sign the Bid on behalf of the Bidder: **[*insert complete name of person duly authorized to sign the Bid*]

Title of the person signing the Bid: [*insert complete title of the person signing the Bid*]

Signature of the person named above: [*insert signature of person whose name and capacity are shown above*]

Date signed [*insert date of signing*] **day of** [*insert month*], [*insert year*]

3. PRICE SCHEDULE FORMS

Notes to Bidders on working with the Price Schedules

General

1. The Price Schedules are divided into separate Schedules as follows:
   - 3.1 Grand Summary Cost Table
   - 3.2 Supply and Installation Cost Summary Table
   - 3.3 Recurrent Cost Summary Table
   - 3.4 Supply and Installation Cost Sub-Table(s)
   - 3.5 Recurrent Cost Sub-Tables(s)
   - 3.6 Country of Origin Code Table

2. The Schedules do not generally give a full description of the information technologies to be supplied, installed, and operationally accepted, or the Services to be performed under each item. However, it is assumed that Bidders shall have read the Technical Requirements and other sections of these bidding documents to ascertain the full scope of the requirements associated with each item prior to filling in the rates and prices. The quoted rates and prices shall be deemed to cover the full scope of these Technical Requirements, as well as overhead and profit.

3. If Bidders are unclear or uncertain as to the scope of any item, they shall seek clarification in accordance with the Instructions to Bidders in the bidding documents prior to submitting their bid.

Pricing

4. Prices shall be filled in indelible ink, and any alterations necessary due to errors, etc., shall be initialed by the Bidder. As specified in the Bid Data Sheet, prices shall be fixed and firm for the duration of the Contract.

5. Bid prices shall be quoted in the manner indicated and in the currencies specified in ITB 18.1 and ITB 18.2. Prices must correspond to items of the scope and quality defined in the Technical Requirements or elsewhere in these bidding documents.

6. The Bidder must exercise great care in preparing its calculations, since there is no opportunity to correct errors once the deadline for submission of bids has passed. A single error in specifying a unit price can therefore change a Bidder's overall total bid price substantially, make the bid noncompetitive, or subject the Bidder to possible loss. The Purchaser will correct any arithmetic error in accordance with the provisions of ITB 32.

7. Payments will be made to the Supplier in the currency or currencies indicated under each respective item. As specified in ITB 18.2, no more than three foreign currencies may be used.

3.1 Grand Summary Cost Table

		*[insert: **Local Currency]*** ***Price***	*[insert: **Foreign Currency A]*** ***Price***	*[insert: **Foreign Currency B]*** ***Price***	*[insert: **Foreign Currency C]*** ***Price***
1.	Supply and Installation Costs (from Supply and Installation Cost Summary Table)				
2.	Recurrent Costs (from Recurrent Cost Summary Table)	Not Applicable			
4.	Grand Totals (to Bid Submission Form)				

Name of Bidder:		
Authorized Signature of Bidder:		

3.2 Supply and Installation Cost Summary Table

Costs MUST reflect prices and rates quoted in accordance with ITB 17 and 18.

			Supply & Installation Prices				
			Locally supplied items	**Items supplied from outside the Purchaser's Country**			
Line Item No.	**Subsystem / Item**	**Supply and Installation Cost Sub-Table No.**	*[insert: **Local Currency]*** Price	*[insert: **Local Currency]*** Price	*[insert: **Foreign Currency A]*** Price	*[insert: **Foreign Currency B]*** Price	*[insert: **Foreign Currency C]*** Price
1	Detailed design of the implementation of the Cyber Attack Simulation						
2	Applications and Security Testing Appliance						
3	Application and Threat Intelligence Program						
4	Application Server						
5	Interfaces						
6	Analog Platform						
7	Server						
8	Workstation						
9	Whiteboard						
10	Monitor						
11	PoE Switch (24 Port)						
12	PoE Switch (48 Port)						
13	Router (Type-1)						
14	Router (Type-2)						

			Supply & Installation Prices				
			Locally supplied items	**Items supplied from outside the Purchaser's Country**			
Line Item No.	**Subsystem / Item**	**Supply and Installation Cost Sub-Table No.**	*[insert: **Local Currency]*** Price	*[insert: **Local Currency]*** Price	*[insert: **Foreign Currency A]*** Price	*[insert: **Foreign Currency B]*** Price	*[insert: **Foreign Currency C]*** Price
15	Network Management System (NMS)						
16	Wireless Location & Wireless Intrusion Prevention System						
17	Virtual Switching Software						
18	Mail Security System						
19	Web Security System						
20	Virtual Firewall						
21	Virtual Instruction Prevention System						
22	End-Point Malware Protection Software						
23	Security Management System						
24	Network Behavior Analysis System						
25	Network Access Control and Authentication System						
26	Wireless Access Point						
27	Hyper-Visor, VDI & Hyper-Visor Management System						
28	SAN Switch						
29	Storage Server						

			Supply & Installation Prices				
			Locally supplied items	**Items supplied from outside the Purchaser's Country**			
Line Item No.	**Subsystem / Item**	**Supply and Installation Cost Sub-Table No.**	*[insert: **Local Currency]*** Price	*[insert: **Local Currency]*** Price	*[insert: **Foreign Currency A]*** Price	*[insert: **Foreign Currency B]*** Price	*[insert: **Foreign Currency C]*** Price
30	Firewall (Type-1)						
31	Firewall (Type-2)						
32	SIEM and Data Analytics System						
33	Industrial Switch (Type-1)						
34	Industrial Switch (Type-2)						
35	Industrial Router						
36	Training Platform Module						
37	Cyber Defence Exercise Module						
38	Center Operations Manual and Self-Organising Capabilities Module						
39	Training Center Operations Functionality Warranty						
40	Automation and Orchestration						
SUBTOTALS							
TOTAL (To Grand Summary Table)							

Note: - - indicates not applicable. "Indicates repetition of table entry above. Refer to the relevant Supply and Installation Cost Sub-Table for the specific components that constitute each Subsystem or line item in this summary table

Name of Bidder:		
Authorized Signature of Bidder:		

3.3 Recurrent Cost Summary Table – Not Applicable

Costs MUST reflect prices and rates quoted in accordance with ITB 17 and ITB 18.

Line Item No.	**Subsystem / Item**	**Recurrent Cost Sub-Table No.**	***[insert: Local Currency] Price***	***[insert: Foreign Currency A] Price***	***[insert: Foreign Currency B] Price***	***[insert: Foreign Currency C] Price***
y	Recurrent Cost Items	Not Applicable				
y.1	____					
	Subtotals (to Grand Summary Table)					

Note: Refer to the relevant Recurrent Cost Sub-Tables for the specific components that constitute the Subsystem or line item in this summary table.

Name of Bidder:		
Authorized Signature of Bidder:		

3.4 Supply and Installation Cost Sub-Table *[insert: identifying number]*

Line item number: *[specify: **relevant line item number from the Supply and Installation Cost Summary Table** (e.g., 1.1)]*

Prices, rates, and subtotals MUST be quoted in accordance with ITB 17 and ITB 18.

				Unit Prices / Rates					**Total Prices**				
				Supplied Locally	**Supplied from outside the Purchaser's Country**				**Supplied Locally**	**Supplied from outside the Purchaser's Country**			
Component No.	**Component Description**	**Country Of Origin Code**	**Quan-tity**	*[Insert: **Local Currency]***	*[Insert: **Local Currency]***	*[Insert: **Foreign Currency A]***	*[Insert **Foreign Currency B]***	*[Insert: **Foreign Currency C]***	*[Insert: **Local Currency]***	*[Insert: **Local Currency]***	*[Insert: **Foreign Currency A]***	*[Insert: **Foreign Currency B]***	*[Insert: **Foreign Currency C]***
1.				- -	- -	- -	- -	- -					
1	Detailed design of the implementation of the Cyber Attack Simulation												
.2.	Applications and Security Testing Appliance												
3.	Application and Threat Intelligence Program												
4	Application Server												
5	Interfaces												
6	Analog Platform												
7	Server												

				Unit Prices / Rates					Total Prices				
				Supplied Locally	Supplied from outside the Purchaser's Country				Supplied Locally	Supplied from outside the Purchaser's Country			
Component No.	**Component Description**	**Country Of Origin Code**	**Quantity**	*[Insert: **Local Currency]***	*[Insert: **Local Currency]***	*[Insert: **Foreign Currency A]***	*[Insert **Foreign Currency B]***	*[Insert: **Foreign Currency C]***	*[Insert: **Local Currency]***	*[Insert: **Local Currency]***	*[Insert: **Foreign Currency A]***	*[Insert: **Foreign Currency B]***	*[Insert: **Foreign Currency C]***
8	Workstation												
9	Whiteboard												
10	Monitor												
11	PoE Switch (24 Port)												
12	PoE Switch (48 Port)												
13	Router (Type-1)												
14	Router (Type-2)												
15	Network Management System (NMS)												
16	Wireless Location & Wireless Intrusion Prevention System												
17	Virtual Switching Software												
18	Mail Security System												
19	Web Security System												

				Unit Prices / Rates					Total Prices				
				Supplied Locally	Supplied from outside the Purchaser's Country				Supplied Locally	Supplied from outside the Purchaser's Country			
Component No.	**Component Description**	**Country Of Origin Code**	**Quantity**	*[Insert: **Local Currency]***	*[Insert: **Local Currency]***	*[Insert: **Foreign Currency A]***	*[Insert **Foreign Currency B]***	*[Insert: **Foreign Currency C]***	*[Insert: **Local Currency]***	*[Insert: **Local Currency]***	*[Insert: **Foreign Currency A]***	*[Insert: **Foreign Currency B]***	*[Insert: **Foreign Currency C]***
20	Virtual Firewall												
21	Virtual Instruction Prevention System												
22	End-Point Malware Protection Software												
23	Security Management System												
24	Network Behavior Analysis System												
25	Network Access Control and Authentication System												
26	Wireless Access Point												
27	Hyper-Visor, VDI & Hyper-Visor Management System												
28	SAN Switch												
29	Storage Server												
30	Firewall (Type-1)												

				Unit Prices / Rates					Total Prices				
				Supplied Locally	Supplied from outside the Purchaser's Country				Supplied Locally	Supplied from outside the Purchaser's Country			
Component No.	Component Description	Country Of Origin Code	Quantity	*[Insert: Local Currency]*	*[Insert: Local Currency]*	*[Insert: Foreign Currency A]*	*[Insert Foreign Currency B]*	*[Insert: Foreign Currency C]*	*[Insert: Local Currency]*	*[Insert: Local Currency]*	*[Insert: Foreign Currency A]*	*[Insert: Foreign Currency B]*	*[Insert: Foreign Currency C]*
31	Firewall (Type-2)												
32	SIEM and Data Analytics System												
33	Industrial Switch (Type-1)												
34	Industrial Switch (Type-2)												
35	Industrial Router												
36	Training Platform Module												
37	Cyber Defence Exercise Module												
38	Center Operations Manual and Self-Organising Capabilities Module												
39	Training Center Operations Functionality Warranty												
40	Automation and Orchestration												
Subtotals (to *[insert:* ***line item***] of Supply and Installation Cost Summary Table)													

Note: - - indicates not applicable. The table may be modified by inserting new rows with new item/component, if deemed necessary

Name of Bidder:		
Authorized Signature of Bidder:		

3.5 Recurrent Cost Sub-Table [*insert: identifying number] -- Warranty Period- **Not Applicable***

Lot number: *[if a multi-lot procurement, insert:* ***lot number,*** *otherwise state* ***"single lot procurement"]***

Line item number**:** *[specify:* ***relevant line item number from the Recurrent Cost Summary Table –*** *(e.g., y.1)]*

Currency: *[specify:* ***the currency of the Recurrent Costs in which the costs expressed in this Sub-Table are expressed****]*

[As necessary for operation of the System, specify: ***the detailed components and quantities in the Sub-Table below for the line item specified above, modifying the sample components and sample table entries as needed.*** *Repeat the Sub-Table as needed to cover each and every line item in the Recurrent Cost Summary Table that requires elaboration.]*

Costs MUST reflect prices and rates quoted in accordance with ITB 17 and ITB 18.

		Maximum all-inclusive costs (for costs in *[insert:* ***currency*** *]*)						
Component No.	Component	Y1	Y2	Y3	Y4	...	Yn	Sub-total for *[insert:* ***currency*** *]*
1.	-	-	-	-	-	-	-	
2.	-	-	-	-	-	-	-	
3.	-	-	-	-	-	-	-	
	-	-	-	-	-	-	-	- -
Cumulative Subtotal (to *[insert:* ***currency***] entry for *[insert:* ***line item*** *]* in the Recurrent Cost Summary Table)								

Name of Bidder:		
Authorized Signature of Bidder:		

3.6 Country of Origin Code Table

Country of Origin	Country Code		Country of Origin	Country Code		Country of Origin	Country Code

Form ELI 2.1.1
Bidder Information Form

[The Bidder shall fill in this Form in accordance with the instructions indicated below. No alterations to its format shall be permitted and no substitutions shall be accepted.]

Date: *[insert date (as day, month and year) of Bid submission*]
RFB No.: *[insert number of Bidding process]*
Alternative No.: *[insert identification No if this is a Bid for an alternative]*

Page _____ of_ _____ pages

1. Bidder's Name *[insert Bidder's legal name]*
2. In case of JV, legal name of each member : *[insert legal name of each member in JV]*
3. Bidder's actual or intended country of registration: *[insert actual or intended country of registration]*
4. Bidder's year of registration: *[insert Bidder's year of registration]*
5. Bidder's Address in country of registration: *[insert Bidder's legal address in country of registration]*
6. Bidder's Authorized Representative Information Name: *[insert Authorized Representative's name]* Address: *[insert Authorized Representative's Address]* Telephone/Fax numbers: *[insert Authorized Representative's telephone/fax numbers]* Email Address: *[insert Authorized Representative's email address]*
7. Attached are copies of original documents of *[check the box(es) of the attached original documents]* ☐ Articles of Incorporation (or equivalent documents of constitution or association), and/or documents of registration of the legal entity named above, in accordance with ITB 4.4. ☐ In case of JV, letter of intent to form JV or JV agreement, in accordance with ITB 4.1. ☐ In case of state-owned enterprise or institution, in accordance with ITB 4.6 documents establishing: • Legal and financial autonomy • Operation under commercial law • Establishing that the Bidder is not under the supervision of the Purchaser ☐ Included are the organizational chart, a list of Board of Directors, and the beneficial ownership.

Form ELI 2.1.2

Bidder's JV Members Information Form

[The Bidder shall fill in this Form in accordance with the instructions indicated below. The following table shall be filled in for the Bidder and for each member of a Joint Venture]].

Date: *[insert date (as day, month and year) of Bid submission*]
RFB No.: *[insert number of Bidding process]*
Alternative No.: *[insert identification No if this is a Bid for an alternative]*

Page _____ of_ _____ pages

1. Bidder's Name: *[insert Bidder's legal name]*
2. Bidder's JV Member's name: *[insert JV's Member legal name]*
3. Bidder's JV Member's country of registration: *[insert JV's Member country of registration]*
4. Bidder's JV Member's year of registration: *[insert JV's Member year of registration]*
5. Bidder's JV Member's legal address in country of registration: *[insert JV's Member legal address in country of registration]*
6. Bidder's JV Member's authorized representative information Name: *[insert name of JV's Member authorized representative]* Address: *[insert address of JV's Member authorized representative]* Telephone/Fax numbers: *[insert telephone/fax numbers of JV's Member authorized representative]* Email Address: *[insert email address of JV's Member authorized representative]*
7. Attached are copies of original documents of *[check the box(es) of the attached original documents]* ☐ Articles of Incorporation (or equivalent documents of constitution or association), and/or registration documents of the legal entity named above, in accordance with ITB 4.4. ☐ In case of a state-owned enterprise or institution, documents establishing legal and financial autonomy, operation in accordance with commercial law, and they are not under the supervision of the Purchaser in accordance with ITB 4.6. ☐ Included are the organizational chart, a list of Board of Directors, and the beneficial ownership.

Form CON – 2

Historical Contract Non-Performance and Pending Litigation

In case a prequalification process was conducted this form should be used only if the information submitted at the time of prequalification requires updating

Bidder's Legal Name: _____ Date: _____

JV member Legal Name: _____ _____

RFB No.: _____

Page _____ of _____ pages

Non-Performing Contracts in accordance with Section III, Evaluation and Qualification Criteria			
Contract non-performance did not occur during the stipulated period, in accordance with Sub- Factor 2.2.1 of Section III, Evaluation Criteria			

Pending Litigation, in accordance with Section III, Evaluation and Qualification Criteria			
No pending litigation in accordance with Sub-Factor 2.2.3 of Section III, Evaluation Criteria Pending litigation in accordance with Sub-Factor 2.2.3 of Section III, Evaluation Criteria, as indicated below			
Year	Outcome as Percent of Total Assets	Contract Identification	Total Contract Amount (current value, US$ equivalent)
_____	_____	Contract Identification: Name of Purchaser: Address of Purchaser: Matter in dispute:	_____
_____	_____	Contract Identification: Name of Purchaser: Address of Purchaser: Matter in dispute:	_____

Form EXP 2.4.1

Experience - General Experience

Bidder's Legal Name: _____ Date: _____

JV Member Legal Name: _____RFB No.: _____

Page _____ of _____ pages

Starting Month / Year	Ending Month / Year	Years *	Contract Identification	Role of Bidder
_____	_____		Contract name: Brief Description of the Information System performed by the Bidder: Name of Purchaser: Address:	_____
_____	_____		Contract name: Brief Description of the Information System performed by the Bidder: Name of Purchaser: Address:	_____
_____	_____		Contract name: Brief Description of the Information System performed by the Bidder: Name of Purchaser: Address:	_____
_____	_____		Contract name: Brief Description of the Information System performed by the Bidder: Name of Purchaser: Address:	_____

Starting Month / Year	Ending Month / Year	Years *	Contract Identification	Role of Bidder
_____	_____		Contract name: Brief Description of the Information System performed by the Bidder: Name of Purchaser: Address:	_____
_____	_____		Contract name: Brief Description of the Information System performed by the Bidder: Name of Purchaser: Address:	_____

*List calendar year for years with contracts with at least nine (9) months activity per year starting with the earliest year

Form EXP – 2.4.2

Specific Experience

Bidder's Legal Name: _____ Date: _____

JV Member Legal Name: _____ RFB No.: _____

Page _____ of _____ pages

Similar Contract Number: ___ of ___ required.	**Information**		
Contract Identification	_____		
Award date Completion date	_____ _____		
Role in Contract	☐ Prime Supplier	☐ Management Contractor	☐ Subcontractor
Total contract amount	_____		US$_____
If member in a JV or subcontractor, specify participation of total contract amount	_____%	_____	US$_____
Purchaser's Name:	_____		
Address: Telephone/fax number: E-mail:	_____ _____ _____ _____		

Form EXP – 2.4.2 (cont.)

Specific Experience (cont.)

Bidder's Legal Name: _____ Page _____ of _____ pages

JV Member Legal Name: _____

Similar Contract No. __[insert specific number] of [total number of contracts] ___ required	**Information**
Description of the similarity in accordance with Sub-Factor 2.4.2 of Section III:	
Amount	_____
Physical size	_____
Complexity	_____
Methods/Technology	_____
Key Activities	_____

Form CCC

Summary Sheet: Current Contract Commitments / Work in Progress

Name of Bidder or partner of a Joint Venture

Bidders and each partner to an Joint Venture bid should provide information on their current commitments on all contracts that have been awarded, or for which a letter of intent or acceptance has been received, or for contracts approaching completion, but for which an unqualified, full completion certificate has yet to be issued.

Name of contract	Purchaser, contac address/tel./fax	Value of outstanding Information System (current US$ equivaler	Estimated completion date	Average monthly invoicing over last s months (US$/month)
1.				
2.				
3.				
4.				
5.				
etc.				

Form FIN – 2.3.1

Financial Situation

Historical Financial Performance

Bidder's Legal Name: _____ Date: _____

JV Member Legal Name: _____ RFB No.: _____

Page _____ of _____ pages

To be completed by the Bidder and, if JV, by each member

Financial information in US$ equivalent	Historic information for previous _____ (__) years (US$ equivalent in 000s)						
	Year 1	Year 2	Year 3	Year …	Year n	Avg.	Avg. Ratio
Information from Balance Sheet							
Total Assets (TA)							
Total Liabilities (TL)							
Net Worth (NW)							
Current Assets (CA)							
Current Liabilities (CL)							
Information from Income Statement							
Total Revenue (TR)							
Profits Before Taxes (PBT)							

Attached are copies of financial statements (balance sheets, including all related notes, and income statements) for the years required above complying with the following conditions:

(a) Must reflect the financial situation of the Bidder or member to a JV, and not sister or parent companies
(b) Historic financial statements must be audited by a certified accountant
(c) Historic financial statements must be complete, including all notes to the financial statements

(d) Historic financial statements must correspond to accounting periods already completed and audited (no statements for partial periods shall be requested or accepted)

Form FIN – 2.3.2

Average Annual Turnover

Bidder's Legal Name: _____ Date: _____

JV Member Legal Name: _____ RFB No.: _____

Page _____ of _____ pages

Annual turnover data (applicable activities only)		
Year	Amount and Currency	US$ equivalent
	_____	_____
	_____	_____
	_____	_____
	_____	_____
	_____	_____
*Average Annual Construction Turnover	_____	_____

*Average annual turnover calculated as total certified payments received for work in progress or completed, divided by the number of years specified in Section III, Evaluation and Qualification Criteria, Sub-Factor 2.3.2.

Form FIN 2.3.3

Financial Resources

Specify proposed sources of financing, such as liquid assets, unencumbered real assets, lines of credit, and other financial means, net of current commitments, available to meet the total construction cash flow demands of the subject contract or contracts as indicated in Section III, Evaluation and Qualification Criteria

Source of financing	Amount (US$ equivalent)
1.	
2.	
3.	
4.	

Personnel Capabilities

Name of Bidder or partner of a Joint Venture

1.	Title of position
	Name of prime candidate
2.	Title of position
	Name of prime candidate
3.	Title of position
	Name of prime candidate
4.	Title of position
	Name of prime candidate

Candidate Summary

Name of Bidder or partner of a Joint Venture

Position		Candidate ☐ Prime ☐ Alternate
Candidate information	Name of candidate	Date of birth
	Professional qualifications	
Present employment	Name of Employer	
	Address of Employer	
	Telephone	Contact (manager / personnel officer)
	Fax	Telex
	Job title of candidate	Years with present Employer

Summarize professional experience over the last twenty years, in reverse chronological order. Indicate particular technical and managerial experience relevant to the project.

From	To	Company/Project/ Position/Relevant technical and management experience

Technical Capabilities

Name of Bidder or partner of a Joint Venture

The Bidder shall provide adequate information to demonstrate clearly that it has the technical capability to meet the requirements for the Information System. With this form, the Bidder should summarize important certifications, proprietary methodologies, and/or specialized technologies that the Bidder proposes to utilize in the execution of the Contract or Contracts.

Manufacturer's Authorization

Note: This authorization should be written on the letterhead of the Manufacturer and be signed by a person with the proper authority to sign documents that are binding on the Manufacturer.

Invitation for Bids Title and No.: *[Purchaser insert: **RFB Title and Number**]*

To: *[Purchaser insert: **Purchaser's Officer to receive the Manufacture's Authorization**]*

WHEREAS *[insert: **Name of Manufacturer**]* who are official producers of *[insert: **items of supply by Manufacturer**]* and having production facilities at *[insert: **address of Manufacturer**]* do hereby authorize *[insert: **name of Bidder or Joint Venture**]* located at *[insert: **address of Bidder or Joint Venture**]* (hereinafter, the "Bidder") to submit a bid and subsequently negotiate and sign a Contract with you for resale of the following Products produced by us:

We hereby confirm that, in case the bidding results in a Contract between you and the Bidder, the above-listed products will come with our full standard warranty.

Name *[insert: **Name of Officer**]* in the capacity of *[insert: **Title of Officer**]*

Signed _____

Duly authorized to sign the authorization for and on behalf of: *[insert: **Name of Manufacturer**]*

Dated this *[insert: **ordinal**]* day of *[insert: **month**]*, *[insert: **year**]*.

[add Corporate Seal (where appropriate)]

Subcontractor's Agreement

Note: This agreement should be written on the letterhead of the Subcontractor and be signed by a person with the proper authority to sign documents that are binding on the Subcontractor.

Invitation for Bids Title and No.: *[Purchaser insert: **RFB Title and Number**]*

To: *[Purchaser insert: **Purchaser's Officer to receive the Subcontractor's Agreement]***

WHEREAS *[insert: **Name of Subcontractor**]*, having head offices at *[insert: **address of Subcontractor**]*, have been informed by *[insert: **name of Bidder or Joint Venture**]* located at *[insert: **address of Bidder or Joint Venture**]* (hereinafter, the "Bidder") that it will submit a bid in which *[insert: **Name of Subcontractor**]* will provide *[insert: **items of supply or services provided by the Subcontractor**]*. We hereby commit to provide the above named items, in the instance that the Bidder is awarded the Contract.

Name *[insert: **Name of Officer**]* in the capacity of *[insert: **Title of Officer]***

Signed _____

Duly authorized to sign the authorization for and on behalf of: *[insert: **Name of Subcontractor**]*

Dated this *[insert: **ordinal**]* day of *[insert: **month**]*, *[insert: **year**]*.

[add Corporate Seal (where appropriate)]

List of Proposed Subcontractors

	Item	Proposed Subcontractor	Place of Registration & Qualifications

INTELLECTUAL PROPERTY FORMS

Notes to Bidders on working with the Intellectual Property Forms

In accordance with ITB 11.1(j), Bidders must submit, as part of their bids, lists of all the Software included in the bid assigned to one of the following categories: (A) System, General-Purpose, or Application Software; or (B) Standard or Custom Software. Bidders must also submit a list of all Custom Materials. These categorizations are needed to support the Intellectual Property in the GCC and SCC.

Software List

	(select one per item)			(select one per item)	
Software Item	System Software	General-Purpose Software	Applicatio Software	Standard Software	Custom Software

List of Custom Materials

Custom Materials

CONFORMANCE OF INFORMATION SYSTEM MATERIALS

Format of the Technical Bid

In accordance with ITB 16.2, the documentary evidence of conformity of the Information System to the bidding documents includes (but is not restricted to):

(a). The Bidder's Preliminary Project Plan, including, but not restricted, to the topics specified in the BDS ITB 16.2. The Preliminary Project Plan should also state the Bidder's assessment of the major responsibilities of the Purchaser and any other involved third parties in System supply and installation, as well as the Bidder's proposed means for coordinating activities by each of the involved parties to avoid delays or interference.

(b). A written confirmation by the Bidder that, if awarded the Contract, it shall accept responsibility for successful integration and interoperability of all the proposed Information Technologies included in the System, as further specified in the Technical Requirements.

(c). Item-by-Item Commentary on the Technical Requirements demonstrating the substantial responsiveness of the overall design of the System and the individual Information Technologies, Goods, and Services offered to those Technical Requirements.

In demonstrating the responsiveness of its bid, the Bidder must use the Technical Responsiveness Checklist (Format). Failure to do so increases significantly the risk that the Bidder's Technical Bid will be declared technically non-responsive. Among other things, the checklist should contain explicit cross-references to the relevant pages in supporting materials included the Bidder's Technical Bid.

Note: The Technical Requirements are voiced as requirements of the *Supplier* and/or the *System*. The Bidder's response must provide clear evidence for the evaluation team to assess the credibility of the response. A response of "yes" or "will do" is unlikely to convey the credibility of the response. The Bidder should indicate *that* – and to the greatest extent practical – *how* the Bidder would comply with the requirements if awarded the contract. Whenever the technical requirements relate to feature(s) of existing products (e.g., hardware or software), the features should be described and the relevant product literature referenced. When the technical requirements relate to professional services (e.g., analysis, configuration, integration, training, etc.) some effort should be expended to describe how they would be rendered – not just a commitment to perform the [cut-and-paste] requirement. If a technical requirement is to provide certifications (e.g., ISO 9001) by the supplier, then copies of the certifications must be included in the Technical Bid.

Note: The Manufacture's Authorizations (and any Subcontractor Agreements) are to be included in Attachment 2 (Bidder Qualifications), in accordance with and ITB 15.

Note: As a matter of practice, the contract cannot be awarded to a Bidder whose Technical Bid deviates (materially) from the Technical Requirements – *on any Technical Requirement*. Such deviations include omissions (e.g., non-responses) and responses that do not meet or exceed the requirement. Extreme care must be exercised in the preparation and presentation of the responses to all the Technical Requirements.

(d). Supporting materials to underpin the Item-by-item Commentary on the Technical Requirements (e.g., product literature, white-papers, narrative descriptions of technical approaches to be employed, etc.). In the interest of timely bid evaluation and contract award, Bidders are encouraged not to overload the supporting materials with documents that do not directly address the Purchaser's requirements.

(e). Any separate and enforceable contract(s) for Recurrent Cost items which the BDS ITB 17.2 required Bidders to bid.

Note: To facilitate bid evaluation and contract award, Bidders encouraged providing electronic copies of their Technical Bid – preferably in a format that the evaluation team can extract text from to facilitate the bid clarification process and to facilitate the preparation of the Bid Evaluation Report.

Technical Responsiveness Checklist (Format)

Tech. Require. No. _	Technical Requirement: *[insert:* ***abbreviated description of Requirement*** *]*
Bidder's technical reasons supporting compliance:	
Bidder's cross references to supporting information in Technical Bid:	

Form of Bid Security (Bank Guarantee)

[The bank shall fill in this Bank Guarantee Form in accordance with the instructions indicated.]

[Guarantor letterhead or SWIFT identifier code]

_____

Beneficiary: *[Purchaser to insert its name and address]* _____

RFB No.: *[Purchaser to insert reference number for the Invitation for Bids]*

Alternative No*.: [Insert identification No if this is a Bid for an alternative]*

Date: _____*[Insert date of issue]* _____

BID GUARANTEE No.: *_[Insert guarantee reference number]*_____

We have been informed that ____ *[insert name of the Bidder, which in the case of a joint venture shall be the name of the joint venture (whether legally constituted or prospective) or the names of all members thereof]* _____ (hereinafter called "the Applicant") has submitted or will submit the Beneficiary its bid _____ (hereinafter called "the Bid") for the execution of _____ under Request for Bids No. _____ ("the RFB").

Furthermore, we understand that, according to the Beneficiary's, Bids must be supported by a Bid guarantee.

At the request of the Applicant, we as Guarantor, hereby irrevocably undertake to pay the Beneficiary any sum or sums not exceeding in total an amount of _____ (_____) upon receipt by us of the Beneficiary's complying demand supported by the Beneficiary's statement, whether in the demand itself or a separate signed document accompanying the demand, stating that either the Applicant:

(a) has withdrawn its Bid during the period of bid validity set forth in the Applicant's Letter of Bid ("the Bid Validity Period"), or any extension thereof provided by the Applicant; or

(b) having been notified of the acceptance of its Bid by the Beneficiary during the period of Bid validity or any extension thereof provided by the Applicant has failed to: (i) execute the Contract Agreement, if required, or (ii) furnish the performance security, in accordance with the Instructions to Bidders ("ITB") of the Beneficiary's bidding document.

This guarantee will expire: (a) if the Applicant is the successful Bidder, upon our receipt of copies of the contract agreement signed by the Applicant and the Performance Security issued to the Beneficiary in relation to such Contract Agreement; or (b) if the Applicant is not the successful Bidder, upon the earlier of (i) our receipt of a copy of the Beneficiary's notification to

the Applicant of the results of the Bidding process; or (ii) twenty-eight days after the expiration of the Bidder's Bid Validity Period.

Consequently, any demand for payment under this guarantee must be received by us at the office on or before that date.

This guarantee is subject to the Uniform Rules for Demand Guarantees (URDG) 2010 Revision, ICC Publication No. 758.

_____

[signature(s)]

Form of Bid Security (Bid Bond) – Not Applicable

BOND NO. _____

BY THIS BOND _____ as Principal (hereinafter called "the Principal"), and _____, **authorized to transact business in** _____, as Surety (hereinafter called "the Surety"), are held and firmly bound unto _____ as Obligee (hereinafter called "the Purchaser") in the sum of _____[1] (_____), for the payment of which sum, well and truly to be made, we, the said Principal and Surety, bind ourselves, our successors and assigns, jointly and severally, firmly by these presents.

WHEREAS the Principal has submitted or will submit a written Bid to the Purchaser dated the ___ day of _____, 20__, for the supply of ___*[name of Contract]* _____ (hereinafter called the "Bid").

NOW, THEREFORE, THE CONDITION OF THIS OBLIGATION is such that if the Principal:

(a) Has withdrawn its Bid during the period of bid validity set forth in the Principal's Letter of of Bid (the Bid Validity Period), or any extension provided by the Principal; or

(b) having been notified of the acceptance of its Bid by the Purchaser during the Bid Validity Period or any extension thereto provided by the Applicant has failed to; (i) execute the Contract Agreement, or (ii) furnish the Performance Security in accordance with the Instructions to Bidders ("ITB") of the Purchaser's bidding document.

then the Surety undertakes to immediately pay to the Purchaser up to the above amount upon receipt of the Purchaser's first written demand, without the Purchaser having to substantiate its demand, provided that in its demand the Purchaser shall state that the demand arises from the occurrence of any of the above events, specifying which event(s) has occurred.

The Surety hereby agrees that its obligation will remain in full force and effect up to and including the date 28 days after the date of expiration of the Bid Validity Period set forth in the Principal's Letter of Bid or extended thereto provided by the Principal.

IN TESTIMONY WHEREOF, the Principal and the Surety have caused these presents to be executed in their respective names this ____ day of _____ 20__.

Principal: _____	Surety: _____ Corporate Seal (where appropriate)
_____ *(Signature)*	_____ *(Signature)*
(Printed name and title)	*(Printed name and title)*

[1] The amount of the Bond shall be denominated in the currency of the *Purchaser*'s Country or the equivalent amount in a freely convertible currency.

Form of Bid-Securing Declaration- Not Applicable

[The Bidder shall fill in this Form in accordance with the instructions indicated.]

Date: *[date (as day, month and year)]*
Bid No.: *[number of bidding process]*
Alternative No.: *[insert identification No if this is a Bid for an alternative]*

To: *[complete name of Purchaser]*

We, the undersigned, declare that:

We understand that, according to your conditions, Bids must be supported by a Bid-Securing Declaration.

We accept that we will automatically be suspended from being eligible for bidding in any contract with the Purchaser for the period of time of *_[number of months or years]* _____, starting on *__[date]*_____, if we are in breach of our obligation(s) under the bid conditions, because we:

(a) have withdrawn our Bid during the period of bid validity specified in the Letter of Bid; or

(b) having been notified of the acceptance of our Bid by the Purchaser during the period of bid validity, (i) fail or refuse to execute the Contract, if required, or (ii) fail or refuse to furnish the Performance Security, in accordance with the ITB.

We understand this Bid-Securing Declaration shall expire if we are not the successful Bidder, upon the earlier of (i) our receipt of your notification to us of the name of the successful Bidder; or (ii) twenty-eight days after the expiration of our Bid.

Name of the Bidder***** _____

Name of the person duly authorized to sign the Bid on behalf of the Bidder****** _____

Title of the person signing the Bid _____

Signature of the person named above _____

Date signed _____ day of _____, _____

*****: In the case of the Bid submitted by joint venture specify the name of the Joint Venture as Bidder

******: Person signing the Bid shall have the power of attorney given by the Bidder attached to the Bid

[Note: In case of a Joint Venture, the Bid-Securing Declaration must be in the name of all members to the Joint Venture that submits the bid.]

SECTION V - ELIGIBLE COUNTRIES

Eligibility for the Provision of Information System

In reference to ITB 4.8 and ITB 5.1, for the information of the Bidders, at the present time firms and information systems from the following countries are excluded from this bidding process:

Under ITB 4.8(a) and ITB 5.1: **Israel**

Under ITB 4.8(b) and ITB 5.1: **None**

SECTION VI - FRAUD AND CORRUPTION

(Section VI shall not be modified)

1. Purpose

1.1 The Bank's Anti-Corruption Guidelines and this annex apply with respect to procurement under Bank Investment Project Financing operations.

2. Requirements

2.1 The Bank requires that Borrowers (including beneficiaries of Bank financing); bidders, consultants, contractors and suppliers; any sub-contractors, sub-consultants, service providers or suppliers; any agents (whether declared or not); and any of their personnel, observe the highest standard of ethics during the procurement process, selection and contract execution of Bank-financed contracts, and refrain from Fraud and Corruption.

2.2 To this end, the Bank:

a. Defines, for the purposes of this provision, the terms set forth below as follows:

i. "corrupt practice" is the offering, giving, receiving, or soliciting, directly or indirectly, of anything of value to influence improperly the actions of another party;

ii. "fraudulent practice" is any act or omission, including misrepresentation, that knowingly or recklessly misleads, or attempts to mislead, a party to obtain financial or other benefit or to avoid an obligation;

iii. "collusive practice" is an arrangement between two or more parties designed to achieve an improper purpose, including to influence improperly the actions of another party;

iv. "coercive practice" is impairing or harming, or threatening to impair or harm, directly or indirectly, any party or the property of the party to influence improperly the actions of a party;

v. "obstructive practice" is:

(a) deliberately destroying, falsifying, altering, or concealing of evidence material to the investigation or making false statements to investigators in order to materially impede a Bank investigation into allegations of a corrupt, fraudulent, coercive, or collusive practice; and/or threatening, harassing, or intimidating any party to prevent it from disclosing its knowledge of matters relevant to the investigation or from pursuing the investigation; or

(b) acts intended to materially impede the exercise of the Bank's inspection and audit rights provided for under paragraph 2.2 e. below.

b. Rejects a proposal for award if the Bank determines that the firm or individual recommended for award, any of its personnel, or its agents, or its sub-consultants, sub-contractors, service providers, suppliers and/ or their employees, has, directly or

indirectly, engaged in corrupt, fraudulent, collusive, coercive, or obstructive practices in competing for the contract in question;

c. In addition to the legal remedies set out in the relevant Legal Agreement, may take other appropriate actions, including declaring misprocurement, if the Bank determines at any time that representatives of the Borrower or of a recipient of any part of the proceeds of the loan engaged in corrupt, fraudulent, collusive, coercive, or obstructive practices during the procurement process, selection and/or execution of the contract in question, without the Borrower having taken timely and appropriate action satisfactory to the Bank to address such practices when they occur, including by failing to inform the Bank in a timely manner at the time they knew of the practices;

d. Pursuant to the Bank's Anti-Corruption Guidelines, and in accordance with the Bank's prevailing sanctions policies and procedures, may sanction a firm or individual, either indefinitely or for a stated period of time, including by publicly declaring such firm or individual ineligible (i) to be awarded or otherwise benefit from a Bank-financed contract, financially or in any other manner;[1] (ii) to be a nominated[2] sub-contractor, consultant, manufacturer or supplier, or service provider of an otherwise eligible firm being awarded a Bank-financed contract; and (iii) to receive the proceeds of any loan made by the Bank or otherwise to participate further in the preparation or implementation of any Bank-financed project;

e. Requires that a clause be included in bidding/request for proposals documents and in contracts financed by a Bank loan, requiring (i) bidders, consultants, contractors, and suppliers, and their sub-contractors, sub-consultants, service providers, suppliers, agents personnel, permit the Bank to inspect[3] all accounts, records and other documents relating to the submission of bids and contract performance, and to have them audited by auditors appointed by the Bank.

---

[1] For the avoidance of doubt, a sanctioned party's ineligibility to be awarded a contract shall include, without limitation, (i) applying for pre-qualification, expressing interest in a consultancy, and bidding, either directly or as a nominated sub-contractor, nominated consultant, nominated manufacturer or supplier, or nominated service provider, in respect of such contract, and (ii) entering into an addendum or amendment introducing a material modification to any existing contract.

[2] A nominated sub-contractor, nominated consultant, nominated manufacturer or supplier, or nominated service provider (different names are used depending on the particular bidding document) is one which has been: (i) included by the bidder in its pre-qualification application or bid because it brings specific and critical experience and know-how that allow the bidder to meet the qualification requirements for the particular bid; or (ii) appointed by the Borrower.

[3] Inspections in this context usually are investigative (i.e., forensic) in nature. They involve fact-finding activities undertaken by the Bank or persons appointed by the Bank to address specific matters related to investigations/audits, such as evaluating the veracity of an allegation of possible Fraud and Corruption, through the appropriate mechanisms. Such activity includes but is not limited to: accessing and examining a firm's or individual's financial records and information, and making copies thereof as relevant; accessing and examining any other documents, data and information (whether in hard copy or electronic format) deemed relevant for the investigation/audit, and making copies thereof as relevant; interviewing staff and other relevant individuals; performing physical inspections and site visits; and obtaining third party verification of information.

PART 2 – PURCHASER'S REQUIREMENTS

SECTION VII - REQUIREMENTS OF THE INFORMATION SYSTEM

(INCLUDING TECHNICAL REQUIREMENTS, IMPLEMENTATION SCHEDULE, SYSTEM INVENTORY TABLES, BACKGROUND AND INFORMATIONAL MATERIALS)

Notes on preparing the Requirements of the Information System

The Requirements of the Information System comprise four significant and closely related subsections:

- *Technical Requirements*
- *Implementation Schedule*
- *System Inventory Tables*
- *Background and Informational Materials*

Each subsection is presented and discussed separately

Technical Requirements

Notes on preparing the Technical Requirements

The Technical Requirements – in combination with the Implementation Schedule and the supporting System Inventory Tables – state the Supplier's obligations to design, supply and install the Information System and, as such, should be "voiced" to the Supplier (i.e., "The System MUST …" "The Supplier MUST …"). They form the contractual basis for the Purchaser-Supplier interactions on technical matters (in combination with refinements introduced through the Supplier's bid, the Project Plan, and any Change Orders).

The Technical Requirements also must include all the technical details that Bidders will need to prepare realistic, responsive, and competitive bids (i.e., covering all their obligations under the Contract if so awarded). However, matters addressed to the Bidder's (i.e., before contract award) generally belong in the Format of the Technical Bid Section 8 of Part 1.

Often Technical Requirements are based on either consultant's project proposals (voiced to the Purchaser's management) or bids from previous procurements (voiced to the Purchaser). In both instances, care needs to be taken in converting these materials into Technical Requirements (voiced to the Supplier). Otherwise, substantial ambiguity will be introduced into the Technical Requirements from, among other things, "aspirational" text suggesting the benefits (to the Purchaser) which are often not obligations that the Supplier can deliver on or be held to deliver upon. Bid based language will often include "sales pitches", such as "expandability up to sixteen processors", whereas the Technical Requirements need to be stated as threshold values to be cleared by the Supplier (e.g., "expandability to at least sixteen processors").

Any sustainable procurement technical requirements shall be clearly specified. Please refer to the Bank's Procurement Regulations for IPF Borrowers and Sustainable procurement guidance notes/tool kit for further information. The sustainable procurement requirements may be specified to enable evaluation of such a requirement on a pass/fail basis and/or rated criteria (point system), as appropriate.

To the greatest extent possible, the Technical Requirements should be expressed in terms of the Purchaser's business activities, rather than a technological design. This leaves it up to the market to determine what specific Information Technologies can best satisfy these business needs. This is particularly relevant where the Information System will embody complex business logic in the form of application software.

Even in the case of a relatively straight-forward Information System, where the business needs can be clearly linked to technological and methodological requirements known in advance of any bidding, the requirements must still be vendor-neutral and admit the widest possible range of technical responses.

Accordingly, references to brand names, catalog numbers, or other details that limit the source of any item or component to a specific manufacturer should be avoided. Where such references are unavoidable, the words "or substantially equivalent" should be added to permit Bidders to bid equivalent or superior technologies. (The Purchaser will need to be ready to indicate how this equivalence will be assessed.) Only in the most exceptional circumstances may Bidders be required to offer brand-name items and the equivalency clause be omitted. The World Bank's consideration for exception requires that:

(a) a brand-name component appears to have no equivalent or superior alternative, because: of its unique ability to reliably interoperate with a relatively large base of existing technologies; to conform with the Purchaser's adopted technological standards; and to offer overwhelming savings in terms of avoided costs for retraining, data conversion, macro / business template redevelopment, etc.;

(b) the World Bank has agreed in advance, during project preparation, that such brand-name restrictions are warranted; and

(c) such brand-name components are the absolute fewest possible and each component has been explicitly identified in the Bid Data Sheet for ITB 16.3 .

Similarly, where national standards or codes of practice are specified, the Purchaser should include a statement that other national or international standards "that are substantially equivalent" will also be acceptable.

To help ensure comparable bids and ease Contract execution, the Purchaser's requirements must be stated as clearly as possible, with minimum room for differing interpretations. Thus, wherever possible, technical requirements should include definitive characteristics and quantifiable measures. If technical characteristics in a specific range, or above or below specific thresholds, are required, then these should be clearly specified. For example, the expandability of a server should be stated as "no less than four processors." Technical specifications that state only "four processors" create unnecessary uncertainty for Bidders regarding whether or not, for example, a server that could be expanded up to six processor boards would be technically responsive.

Quantitative technical specifications must, however, be employed with care. They can dictate technical architectures and, thus, be unnecessarily restrictive. For example, a quantitative requirement for the minimum width of the data path in a processor may be unnecessarily restrictive. Instead, a specification of a required level of standard performance benchmark test is more appropriate, allowing different technical approaches to achieving the Purchaser's functional and performance objectives. In general, the Purchaser should try to use widely accepted direct measures of performance and functionality whenever possible and carefully review specifications for those that might dictate technical architectures.

It is important that the Technical Requirements clearly identify which are mandatory features (for which a bid's nonconformance might require rejection for non-responsiveness) and which are preferable features that can be included or excluded from a bid at the Bidder's option. To enhance the clarity of the specifications, Purchasers are advised to use the word "MUST" (in bold capitals) in sentences describing mandatory requirements. A clear requirements numbering scheme is also essential.

The following presents a sample outline format for the Technical Requirements Section. This can and should be adapted to meet the Purchaser's needs for the specific Information System to be procured.

Technical Requirements

Table of Contents: Technical Requirements

A. ACRONYMS USED IN THE TECHNICAL REQUIREMENTS

0.1 Acronym Table

Numeric	
I x RTT	one times radio transmission technology
3DES	Triple Data Encryption Standard
3G	3rd Generation
3GPP	3rd Generation Partnership Project
3GPP2	3rd Generation Partnership Project 2
4G	4th Generation
A	
AA	ABAC attribute authority
AAA	authentication, authorization, and accounting
AAAK	authentication, authorization, and accounting key
AAD	additional authenticated data
AAR	after action report
ABAC	attribute-based access control
ACE	access control entry
ACL	access control list
ACO	authenticated cipher offset
AD	Active Directory
AD	authenticated data
ADS	alternate data stream
AES	Advanced Encryption Standard
AES-CBC	Advanced Encryption Standard-Cipher Block Chaining
AES-CTR	Advanced Encryption Standard-Counter Mode
AFH	adaptive frequency hopping
A-GPS	assisted global positioning system
AH	Authentication Header
AIDC	automatic identification and data capture
AIT	automatic identification technology
AJAX	Asynchronous JavaScript and XML
AK	authorization key
AKID	authorization key identifier
AKM	authentication and key management
ALG	application layer gateway
ANSI	American National Standards Institute
AP	access point
API	application programming interface
APWG	Anti-Phishing Working Group
ARIN	American Registry for Internet Numbers
ARP	Address Resolution Protocol
ARPA	Advanced Research Projects Agency
AS	authentication server
AS	authentication service
AS	autonomous system
ASC	Anti-Spyware Coalition
ASC X9	Accredited Standards Committee X9
ASCII	American Standard Code for Information Interchange
ASLR	address space layout randomization
ASN	autonomous system number
ASN.1	Abstract Syntax Notation 1

ASP	active server pages
ATA	Advanced Technology Attachment
ATA	Advanced Threat Analytics
ATEVI	Announcement Traffic Indication Message
ATM	asynchronous transfer mode
ATM	automated teller machine
AV	antivirus
AVIEN	Anti-Virus Information Exchange Network
AVP	attribute-value pair
B	
B2B	business-to-business
BCP	best current practice
BCP	business continuity plan
BGP	Border Gateway Protocol
BGP-4	Border Gateway Protocol 4
BIA	Bump-in-the-API
BIA	business impact analysis
BioAPI	Biometric Application Programming Interface
BIOS	basic input/output system
BITS	Bump-in-the-Stack
BPML	Business Process Modeling Language
BPSS	Business Process Specification Schema
BRP	business recovery (resumption) plan
BS	base station
BSC	base station controller
BSI	British Standards Institution
BSIA	British Security Industry Association
BSP	best security practice
BSS	basic service set
BSSID	basic service set identifier
BTNS	better-than-nothing-security
BTS	base transceiver station
BU	binding update
C	
C&A	certification and accreditation
CA	certificate authority
CA	certification agent
CA	certification authority
CAC	common access card
CAIDA	Cooperative Association for Internet Data Analysis
CAPTCHA	Completely Automated Public Turing Test to Tell Computers and Humans Apart
CARO	Computer Antivirus Research Organization
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CBC-MAC	Cipher Block Chaining Message Authentication Code
CBEFF	Common Biometric Exchange File Format
CC	Common Criteria
CCETM	Common Configuration Enumeration
CCEVS	Common Criteria Evaluation and Validation Scheme
CCIPS	Computer Crime and Intellectual Property Section
CCK	complementary code keying
CCM	Counter Mode with CBC-MAC
CCMP	Counter Mode with CBC-MAC Protocol
CCRA	Common Criteria Recognition Arrangement
CCSS	Common Configuration Scoring System

CcTLD	country code top-level domain
CD	checking disabled
CERT	computer emergency response team
CERT®/CC	CERT® Coordination Center
CF	CompactFlash®
CFAA	Computer Fraud and Abuse Act
CFB	Cipher Feedback
CFI	computer and financial investigations
CFR	Code of Federal Regulations
CFTT	computer forensics tool testing
CGA	cryptographically generated addresses
CGI	Common Gateway Interface
CHAP	Challenge-Handshake Authentication Protocol
CHUID	cardholder unique identifier
CIDR	Classless Inter-Domain Routing
CIFS	Common Internet File System
CIP	critical infrastructure protection
CIPC	Critical Infrastructure Protection Committee
CIPSEA	Confidential Information Protection and Statistical Efficiency Act
CIRC	computer incident response capability
CIRC	computer incident response center
CIRDB	CERIAS Incident Response Database
CIRT	computer incident response team
CIS	Center for Internet Security
CISO	chief information security officer
CLF	common log format
CLI	command Line Interface
CLR	common language runtime
CMA	Certificate Management Authority
CMAC	Cipher-based Method Authentication Code
CME	Common Malware Enumeration
CMS	Cryptographic Message Syntax
CMVP	Cryptographic Module Validation Program
CN	common name
CN	correspondent node
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
CoA	care-of address
Codec	coder/decoder
COI	conflict of interest
COM	Component Object Model
COOP	continuity of operations
COPPA	Children's Online Privacy Protection Act
CORBA®	Common Object Request Broker Architecture
COTS	commercial off-the-shelf
CP	certificate policy
CP	contingency plan
CPETM	Common Platform Enumeration
CPI	compression parameter index
CPNI	Centre for the Protection of National Infrastructure
CPS	certification practice statement
CRAM	challenge response authentication mechanism
CRC	cyclic redundancy check
CRL	certificate revocation list
CSIRC	computer security incident response capability
CSIRT	computer security incident response team

CSO	chief security officer
CSO	computer security object
CSP	Credentials Service Provider
CSR	certificate signing request
CSRC	Computer Security Resource Center
CSS	cascading style sheet
CSV	comma-separated values
CTR	counter mode encryption
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
CWE	Common Weakness Enumeration
D	
DA	destination address
DAA	designated accrediting authority
DAA	designated approving authority
DAC	discretionary access control
DAD	duplicate address detection
DAML	DARPA Agent Markup Language
D-AMPS	Digital Advanced Mobile Phone Service
DAD	Data Access Object
DBMS	database management system
DC	domain controller
DCE	Distributed Computing Environment
DCOM	Distributed Component Object Model
DCS	distributed control system
DDoS	distributed denial of service
DEA	Data Encryption Algorithm
DEP	Data Execution Prevention
DES	Data Encryption Standard
DFS	Distributed File System
DFS	dynamic frequency selection
DH	Diffie-Hellman
DHAAD	Dynamic Home Agent Address Discovery
DHCP	Dynamic Host Configuration Protocol
DHCPv6	Dynamic Host Configuration Protocol for Internet Protocol v6
DIMS	Digital Identity Management Service
DLL	dynamic link library
DMA	direct memory access
DMZ	demilitarized zone
DN	distinguished name
DN	domain name
DNP	Distributed Network Protocol
DNS	domain name system
DNSBL	Domain Name System Blacklist
DNSSEC	Domain Name System Security Extensions
DOI	domain of interpretation
DOM	Document Object Model
DoS	denial of service
DPA	differential power analysis
DRA	data recovery agent
DRM	digital rights management
DRP	disaster recovery plan
DS	Delegation Signer
DS	distribution system
DS Field	differentiated services field
DSA	Digital Signature Algorithm

DSL	digital subscriber line
DSML	Directory Services Markup Language
DSN	delivery status notification
DSOD	dynamic separation of duty
DSS	Digital Signature Standard
DSTM	Dual Stack Transition Mechanism
DTC	Distributed Transaction Coordinator
DTD	Document Type Definition
DTR	derived test requirement
DUID	DHCP unique identifier
E	
EAL	evaluation assurance level
EAP	Extensible Authentication Protocol
EAP-FAST	Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling
EAPOL	Extensible Authentication Protocol over LAN
EAPOL-KCK	Extensible Authentication Protocol over LAN Key Confirmation Key
EAPOL-KEK	Extensible Authentication Protocol over LAN Key Encryption Key
EAP-TLS	Extensible Authentication Protocol-Transport Layer Security
EAP-TTLS	Extensible Authentication Protocol-Tunneled Transport Layer Security
EBGP	Exterior Border Gateway Protocol
ECB	Electronic Codebook (mode)
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
ECM	Enterprise Configuration Manager
ECP	Encryption Control Protocol
EDGE	Enhanced Data rates for GSM Evolution
EDI	electronic data interchange
EDR	enhanced data rate
EEPROM	electronically erasable programmable read-only memory
EFI	Extensible Firmware Interface
EFS	Encrypting File System
EGP	Exterior Gateway Protocol
EH	extension header
EICAR	European Institute for Computer Antivirus Research
EIGRP	Enhanced Interior Gateway Routing Protocol
EIK	EAP Integrity Key
Email	electronic mail
EMS	Enterprise Management System
EMS	Enhanced Messaging Service
EMSK	Extended Master Session Key
EPAL	Enterprise Privacy Authorization Language
EPC	electronic product code
EPCIS	Electronic Product Code Information Services
EPHI	electronic protected health information
EPS	events per second
ERP	enterprise resource planning
ESMS	enterprise security management system
ESMTP	Extended Simple Mail Transfer Protocol
ESN	electronic serial number
ESP	Encapsulating Security Payload
ESS	Extended Service Set
EUI-64	Extended Unique Identifier 64 bit
EV-DO	Evolution-Data Optimized
F	

FAT	file allocation table
FCL	final checklist list
FCS	frame check sequence
FDE	full disk encryption
FEK	file encryption key
FHSS	frequency hopping spread spectrum
FIB	forwarding information base
FIRST	Forum of Incident Response and Security Teams
FMR	false match rate
FNMR	false non match rate
FQDN	fully qualified domain name
FRR	false rejection rate
FSO	field security office
FTP	File Transfer Protocol
FUS	Fast User Switching
G	
GB	gigabyte
GFAC	generalized framework for access control
GFIRST	Government Forum of Incident Response and Security Teams
GHz	gigahertz
GIG	Global Information Grid
GINA	graphical identification and authentication
GKEK	Group Key Encryption Key
GLB *or* GLBA	Gramm-Leach-Bliley Act
GMK	Group Master Key
GnuPG	GNU Privacy Guard
GOTS	government off-the-shelf
GPL	general public license
GPMC	Group Policy Management Console
GPO	Group Policy Object
GPRS	general packet radio service
GPS	global positioning system
GR	graceful restart
GRE	Generic Routing Encapsulation
GRS	General Records Schedule
GS1	Global Standards One
GSM	Global System for Mobile Communications
GTC	Generic Token Card
GTEK	group traffic encryption key
GTK	group temporal key
gTLD	generic top-level domain
GTSM	Generalized TTL Security Mechanism
GUI	graphical user interface
H	
HA	high availability
HAG	high assurance guard
HCI	host controller interface
HERF	hazards of electromagnetic radiation to fuel
HERO	hazards of electromagnetic radiation to ordnance
HERP	hazards of electromagnetic radiation to personnel
HF	high frequency
HFS	Hierarchical File System
HINFO	host information
HIP	Host Identity Protocol
HIPAA	Health Insurance Portability and Accountability Act
HIPERLAN	high-performance radio local area network

HKLM	HKEY Local Machine
HMAC	keyed-hash message authentication code
HMI	human-machine interface
HPA	host protected area
HPFS	High-Performance File System
HTCIA	High Technology Crime Investigation Association
HTCP	Hyper Text Caching Protocol
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Secure Hypertext Transfer Protocol
Hz	hertz
I	
I&A	identification and authentication
I/O	input/output
I3P	Institute for Information Infrastructure Protection
IA	information assurance
IAB	Internet Architecture Board
IACIS®	International Association of Computer Investigative Specialists
IMP	Information Analysis and Infrastructure Protection
IANA	Internet Assigned Numbers Authority
IA0	information assurance officer
IATF	Information Assurance Technical Framework
IBC	iterated block cipher
IBE	identity-based encryption
iBGP	Internal Border Gateway Protocol
IBMJSSE	IBM Java Secure Socket Extension
IBSS	independent basic service set
IC3	Internet Crime Complaint Center
ICAMP	Incident Cost Analysis and Modeling Project
ICANN	Internet Corporation for Assigned Names and Numbers
ICCID	Integrated Circuit Card Identification
ICCP	Inter-control Center Communications Protocol
ICF	Internet Connection Firewall
ICMP	Internet Control Message Protocol
ICP	Internet Cache Protocol
ICS	industrial control system
ICS	Internet Connection Sharing
ICSA	International Computer Security Association
ICV	integrity check value
ID	identification
IDARTrm	Information Design Assurance Red Team
IDE	integrated development environment
IDE	Integrated Drive Electronics
IDEA	International Data Encryption Algorithm
iDEN	Integrated Digital Enhanced Network
ID-FF	Identity Federation Framework
IDMEF	Intrusion Detection Message Exchange Format
IDMS	identity management system
IDPS	intrusion detection and prevention system
IDS	intrusion detection system
ID-SIS	Identity Service Interface Specifications
ID-WSF	Identity Web Services Framework
ID-WSF DST	Identity Web Services Framework Data Services Template
IE	Internet Explorer
IEC	International Electrotechnical Commission
IED	intelligent electronic device

IEEE-SA	IEEE Standards Association
IESG	Internet Security Steering Group
IETF	Internet Engineering Task Force
IETF BCP	Internet Engineering Task Force Best Current Practice
IETF RFC	Internet Engineering Task Force Request for Comments
IGMP	Internet Group Management Protocol
IGP	interior gateway protocol
ID	interface identifier
IIF	information in identifiable form
IIHI	individually identifiable health information
IIS	Internet Information Services
IKE	Internet Key Exchange
IM	instant messaging
IMAP	Internet Message Access Protocol
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
INCITS	International Committee for Information Technology Standards
IP	Internet Protocol
IPA	initial privacy assessment
IPComp	Internet Protocol Payload Compression Protocol
IPng	Internet Protocol Next Generation
IPS	intrusion prevention system
IPsec	Internet Protocol Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IPX	Internet Packet Exchange
IR	infrared
IR	interagency report
IRC	Internet Relay Chat
IrDA®	Infrared Data Association®
IRQ	interrupt request line
IRS	Internal Revenue Service
IRTF	Internet Research Task Force
IS	information system
ISA	interconnection security agreement
ISA	International Society of Automation
ISAC	information sharing and analysis center
ISAKMP	Internet Security Association and Key Management Protocol
ISAP	Information Security Automation Program
ISAPI	Internet Server Application Programming Interface
ISATAP	Intra-Site Automatic Tunnel Addressing Protocol
ISF	Information Security Forum
ISID	Industrial Security Incident Database
IS-IS	Intermediate System-to-Intermediate System
ISM	industrial, scientific, and medical
ISM	information security marking
ISMS	information security management system
ISO	International Organization for Standardization
ISP	Internet service provider
ISSEA	International Systems Security Engineering Association
ISSO	information systems security officer
ISSPM	information systems security program manager
ITU	International Telecommunications Union
ITU-T	International Telecommunications Union-Telecommunication Standardization Sector
IUT	implementation under test
IV	initialization vector

J

Java EE	Java Platform, Enterprise Edition
JAXR	Java API for XML Registries
JFFS2	Journaling Flash File System, version 2
JPEG	Joint Photographic Experts Group
JRE	Java Runtime Environment
JSM	Java Security Manager
JSP	Java Server Pages
JSSE	Java Secure Socket Extension
JTAG	Joint Test Action Group
JTC1	Joint Technical Committee 1 (International Organization for Standardization [ISO] / International Electrotechnical Commission [1EC])
JVM	Java Virtual Machine

K

KB	kilobyte
Kbps	kilobit per second
KDC	key distribution center
KEK	key encryption key
KG	key generator
KGD	key generation and distribution
KHz	kilohertz
KINK	Kerberized Internet Negotiation of Keys
KSG	key stream generator
KSK	key signing key

L

L2CAP	Logical Link Control and Adaptation Protocol
L2F	Layer 2 Forwarding
L2TP	Layer 2 Tunneling Protocol
L2VPN	Layer 2 Virtual Private Network
L3VPN	Layer 3 Virtual Private Network
LACNIC	Latin American and Caribbean IP Addresses Registry
LAN	local area network
LCD	liquid crystal display
LDA	local delivery agent
LDAP	Lightweight Directory Access Protocol
LED	light emitting diode
LF	low frequency
LFSR	linear feedback shift register
LIR	local Internet registry
LMP	Link Manager Protocol
LOC	location (DNS record)
LOS	line-of-sight
LRA	Local Registration Authority
LUA	limited user account

M

MAC	mandatory access control
MAC	media access control (layer)
MAC	Medium Access Control
MAC	message authentication code
MAF	multi-mode authentication framework
MAN	metropolitan area network
MAPS	Mail Abuse Prevention System
MB	megabyte
Mbps	megabits per second
MBR	master boot record
MBSA	Microsoft Baseline Security Analyzer

MD	message digest
ME	mobile equipment
MED	multi-exit discriminator
MEP	message exchange pattern
MES	manufacturing execution system
MHz	megahertz
MIB	management information base
MIC	mandatory integrity control
MIC	message integrity check
MIC	message integrity code
MIKEY	Multimedia Internet KEYing
MIME	Multipurpose Internet Mail Extensions
MIMO	multiple-input, multiple-output
MIN	mobile identification number
Mini SD	mini secure digital
MIP	Mobile Internet Protocol
MitM	man-in-the-middle (attack)
MLD	Multicast Listener Discovery
MMC	Microsoft Management Console
MMC	Multi Media Card
MMCmobile	Multi Media Card Mobile
MMS	Multimedia Messaging Service
MN	mobile node
MO	magneto-optical
MOA	memorandum of agreement
MOBIKE	IKEv2 Mobility and Multi-homing Protocol
MODP	modular exponential
MOSS	MIME Object Security Services
MOU	memorandum of understanding
MOVS	Modes of Operation Validation System
MPA	Mobile Prefix Advertisement
MPLS	multi protocol label switching
MPS	Mobile Prefix Solicitation
MS	mobile subscriber
MSC	mobile switching center
MS-CHAP	Microsoft Challenge Handshake Authentication Protocol
MSDP	Multicast Source Discovery Protocol
MSEC	multi cast security
MSK	master session key
MSSP	managed security services provider
MSWG	Metadata Standards Working Group
MTA	mail transfer agent
MTM	Mobile Trusted Module
MTU	master telemetry unit
MTU	master terminal unit
MTU	maxi mum transmission unit
MUA	mail user agent
MX	mail exchanger
N	
NA	Neighbor Advertisement
NAC	network access control
NAP	Network Access Protection
NAS	network access server
NAT	network address translation
NAT-PT	network address translation—protocol translation
NAT-T	network address translation traversal

NBA	network behavior analysis
NBAD	network behavior anomaly detection
NCES	Net Centric Enterprise Services
ND	Neighbor Discovery
NDAC	nondiscretionary access control
NetBEUI	NetBIOS Extended User Interface
NetBIOS	Network Basic Input / Output System
NetBT	NetBIOS over TCP/IP
NFAT	network forensic analysis tool
NFC	near field communication
NFS	network file system
NFS	Network File Sharing
NH	next header
NIS	Network Information System
NIST	National Institute of Standards and Technology
NLOS	non-line-of-sight
NPPI	nonpublic personal information
NS	name server
NS	Neighbor Solicitation
NSEC	Next Secure
NX	no execute
0	
OCSP	Online Certificate Status Protocol
OEM	original equipment manufacturer
OFB	output feedback (mode)
OFDM	orthogonal frequency-division multiplexing
OGSATM	Open Grid Services Architecture
OHA	Open Handset Alliance
OLE	object linking and embedding
ONS	Object Naming Service
00B	out-of-band
OPC	OLE for Process Control
OpenPGP	Open Specification for Pretty Good Privacy
ORB	open relay blacklist
OS	operating system
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
OSS	open source software
OS ST1VINI	Open Source Security Testing Methodology Manual
OSVDB	Open Source Vulnerability Database
OTP	one-time password
OU	organizational unit
OVAL	Open Vulnerability and Assessment Language
OWASP	Open Web Application Security Project
OWL-S	Web Ontology Language for Services
P	
P2P	peer-to-peer
PAC	Privilege Attribute Certificate
PAC	Protected Access Credential
PAD	peer authorization database
PAM	pluggable authentication module
PAN	personal area network
PAOS	Reverse HTTP Binding for SOAP
PAP	Password Authentication Protocol
PAP	policy access point
PAS	publicly available specification

PBA	pre-boot authentication
PBAC	policy-based access control
PBCC	Packet Binary Convolutional Code
BE	pre-boot environment
PBX	private branch exchange
PC	personal computer
PCI	Payment Card Industry
PCI	personal identity verification card issuer
PCI DSS	Payment Card Industry Data Security Standard
PCMCIA	Personal Computer Memory Card International Association
PCN	process control network
PCP	Payload Compression Protocol
PCS	process control system
PCSF	Process Control System Forum
PCSRF	Process Control Security Requirements Forum
PDA	personal digital assistant
PDD	Presidential Decision Directive
PDF	Portable Document Format
PDP	policy decision point
PDS	protective distribution systems
PEAP	Protected Extendable Authentication Protocol
PED	portable electronic devices
PEM	Privacy Enhanced Mail
PEP	policy enforcement point
PFS	perfect forward secrecy
PGP	Pretty Good Privacy
PHI	protected health information
PHP	PHP: Hypertext Preprocessor
PHY	Physical (layer)
PIA	privacy impact assessment
PIN	personal identification number
PIR	Public Interest Registry
PIV	personal identity verification
PKCS	Public Key Cryptography Standard
PKI	public key infrastructure
PKM	privacy key management
PKMv1	Privacy Key Management Protocol version 1
PKMv2	Privacy Key Management Protocol version 2
PN	packet number
PNG	Portable Network Graphics
POA&M	plan of action and milestones
POC	point of contact
POC	proof of concept
PoE	Power over Ethernet
POP	Post Office Protocol
POP3	Post Office Protocol version 3
PP	protection profile
PPP	Point-to-Point Protocol
PPTP	Point-to-Point Tunneling Protocol
PPVPN	provisioner-provided virtual private network
PRA	Paperwork Reduction Act
Pre-PAK	pre-primary authorization key
PRF	pseudorandom function
PRNG	pseudorandom number generator
PSK	pre-shared key
PSTN	public switched telephone network

PTA	privacy threshold assessment (or analysis)
PTK	pairwise transient key
PTV	perceived target value
PUB	publication
PUK	PIN unblocking key
PVG	patch and vulnerability group
Q	
QoP	quality of protection
QoS	quality of service
R	
R&D	research and development
R/W	read/write
RA	receiver address
RA	Registration Authority
RA	remote assistance
RA	Router Advertisement
RADAC	risk adaptive access control
RADIUS	Remote Authentication Dial In User Service
RAID	redundant array of independent disks
RAM	random access memory
RAT	remote administration tool
RBAC	role-based access control
RC2	Rivest Cipher 2
RC4	Rivest Cipher 4
RCE	route cache entry
RCFL	Regional Computer Forensics Laboratory
RCP	Remote Copy Protocol
RDBMS	relational database management system
RDP	Remote Desktop Protocol
REL	rights expression language
REP	Robots Exclusion Protocol
REST	Representational State Transfer
RF	radio frequency
RFC	request for comments
RFD	route flap damping
RFID	radio frequency identification
RFP	request for proposal
RIB	routing information base
RIP	Routing Information Protocol
RIPng	Routing Information Protocol next generation
RIR	regional internet registries
RIS	Remote Installation Services
RMA	reliability, maintainability, and availability
RMON	Remote Monitoring
RNG	random number generator
ROE	rules of engagement
ROM	read-only memory
RP	responsible person (record)
RPC	remote procedure call
RPF	Reverse Path Forwarding
RPO	recovery point objective
RR	resource record
RRSIG	resource record signature
RS	relay station
RS	Router Solicitation
RSA	Rivest-Shamir-Adelman

RSBAC	rule set-based access control
RSN	Robust Security Network
RSNA	Robust Security Network Association
RSNIE	Robust Security Network Information Element
RSO	reduced sign-on
RSS	Really Simple Syndication
RSSI	received signal strength indication
RSVP	Resource ReserVation Protocol
RTF	Rich Text Format
RTLS	real-time location system
RTO	recovery time objective
RTP	Real-Time Transport Protocol
RTU	remote terminal unit or remote telemetry unit
RuBAC	rule-based access control
R-ULVI	Removable User Identity Module
S	
S/MIME	Secure/Multipurpose Internet Mail Extensions
SA	security association
SA	source address
SACL	system access control list
SAD	security association database
SAFER	Secure and Fast Encryption Routine
SAID	security association identifier
SAISO	senior agency information security officer
SAM	Security Account Manager
SAM	software asset management
SAMATE	Software Assurance Metrics and Tool Evaluation
SAMLTM	Security Assertion Markup LanguageTM
SAN	storage area network
S-BGP	Secure Border Gateway Protocol
SCADA	supervisory control and data acquisition
SCAP	Security Content Automation Protocol
SCP	Secure Copy Protocol
SCSI	Small Computer System Interface
SCTP	Stream Control Transmission Protocol
SD	Secure Digital
SDIO	Secure Digital Input Output
SDK	software development kit
SDLC	System Development Life Cycle
SDO	standards development organization
SDP	Session Description Protocol
SDP	Service Discovery Protocol
SEI	Software Engineering Institute
SEM	security event management
SEND	Secure Neighbor Discovery
SEP	secure entry point
SIEM	security information and event management
SFTP	Secure FiIe Transfer Protocol
SHA	Secure Hash Algorithm
SHA-1	Secure Hash Algorithm 1
SHS	Secure Hash Standard
SIA	Security Industry Association
SID	security identifier
SIG	special interest group
SHT	Stateless IP/ICMP Translation Algorithm
SIM	security information management

SIM	subscriber identity module
SIP	Session Initiation Protocol
SIS	safety instrumented system
SKEME	Secure Key Exchange Mechanism
SLA	service level agreement
SMB	Server Message Block
SME	subject matter expert
SMS	Short Message Service
SMS	Systems Management Server
SMT	scar, mark and tattoo
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SOA	service-oriented architecture
SOA	start of authority (resource record)
SoBGP	Secure Origin Border Gateway Protocol
SoD	separation of duties
SOHO	small office/home off ice
SOP	standard operating procedure
SOR	system of records
SORN	system of records notice
SOX	Sarbanes-Oxley Act
SP	service pack
SP	special publication
SPD	security policy database
SPI	security parameters index
SPL	Structured Product Labeling
SPMLTm	Service Provisioning Markup LanguageTM
SPP-ICS	System Protection Profile for Industrial Control Systems
SQL	Structured Query Language
SR	service release
SRES	signed response
SRTP	Secure Real -Time Transport Protocol
SS	subscriber station
SSDP	Simple Service Discovery Protocol
SSE-CMM	Systems Security Engineering Capability Maturity Model
SSH	Secure Shell
SSID	service set identifier
SSL	Secure Sockets Layer
SSO	single sign-on
SSoD	static separation of duty
SSP	secure simple paring
SSPI	Security Support Provider Interface
ST	security target
STA	station
STIG	security technical implementation guide
STS	security token service
SUID	Set-User-I D
SWSA	Semantic Web Services Initiative Architecture
SZ	security zone
T	
TA	test assertion
TA	transmitter address
TACACS	Terminal Access Controller Access Control System
TAG	technical advisory group
TB	terabyte

TC	technical committee
TC68	ISO/IEC Technical Committee 68
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TDEA	Triple Data Encryption Algorithm
TDM	time division multiplexing
TDMA	time division multiple access
TEK	traffic encryption key
TERENA	Trans-European Research and Education Networking Association
TFT	thin film transistor
TFTP	Trivial File Transfer Protocol
TGS	ticket-granting service
TIA®	Telecommunications Industry Association
TK	temporal key
TKIP	Temporal Key Integrity Protocol
TLD	top-level domain
TLS	Transport Layer Security
TOE	target of evaluation
TOS	trusted operating system
ToS	Type of Service
TPC	transmission power control
TPM	trusted platform module
TR	technical report
TRT	transport relay translator
TS	technical specification
TSA	time stamping authority
TSIG	Secret Key Transaction Authentication for DNS
TSIG	Transaction Signature
TSN	transitional security network
TSP	Time-Stamp Protocol
TT&E	test, training, and exercise
TTF	tag talks first
TTL	time to live
TTLS	Tunneled Transport Layer Security
TTP	trusted third party
TXT	text (record)
U	
UAC	User Account Control
UART	universal *asy*nchronous receiver/transmitter
UCC	Uniform Code Council, Inc.
UCE	unsolicited commercial email
UDDITM	Uniform Description, Discovery, and Integration TM
UDF	Universal Disk Format
UDP	User Datagram Protocol
UFS	UNIX File System
UHF	ultra high frequency
UI	user interface
UL	Underwriters' Laboratories®
ULA	unique local address
ULP	upper layer protocol
UML®	Unified Modeling Language
UMPC	Ultra-mobile personal computer
UMTS	Universal Mobile Telecommunications System
UNIT	Unlicensed National Information Infrastructure
UPC	Universal Product Code
UPnP	Universal Plug and Ray

UPS	uninterruptible power supply
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
USB	Universal Serial Bus
UTM	Unified threat management
V	
VB	Visual Basic
VB.NET	Visual Basic .NET
VBA	Visual Basic f or Applications
VBScript	Visual Basic Script
VFD	variable frequency drive
VHD	virtual hard drive
VHF	very high frequency
VLAN	virtual Local area network
VM	virtual machine
VMS	vulnerability management system
VoIP	V*oice over* Internet Protocol
VOIPSA	Voice over IP Security Alliance
VPN	virtual private network
VPNC	Virtual Private Network Consortium
VRRP	Virtual Router Redundancy Protocol
W	
W3C®	World Wide Web Consortium
WAN	wide area network
WAP	wireless access point
WAP	Wireless Application Protocol
WAYF	Where Are You From
WCCP	Web Cache Coordination Protocol
W-CDMA	Wideband Code Division Multiple Access
WDS	wireless distribution system
WebDAV	Web Distributed Authoring and Versioning
WEP	Wired Equivalent Privacy
WfMC	Workflow Management Coalition
WfMS	workflow management system
WG	working group
WIDPS	wireless intrusion detection and prevention system
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	wireless local area network
WMAN	wireless metropolitan area network
WMM®	Wi-Fi Multimedia
WORM	write once, read many
WPA	Wi-Fi Protected Access
WPA2®	Wi-Fi Protected Access 2
WPAN	wireless personal area network
WS	Web services
WSDL	Web Services Description Language
WSH	Windows Script Host
WS-/	Web services interoperability
WS-/	Web Services Interoperability Organization
WSS4J	Web Services Security for Java
WS-Security	Web Services Security
WSUS	Windows Server Update Services
WVE	Wireless Vulnerabilities and Exploits
WWAN	wireless wide area network
WWW	World Wide Web

XYZ

XACL	XML Access Control Language
XACMLTM	eXtensible Access Control Markup LanguageTM
XCBC	XOR Cipher Block Chaining
XCCDF	eXtensible Configuration Checklist Description Format
XHTML	Extensible Hypertext Markup Language
XKMS	XML Key Management Specification
XML	Extensible Markup Language
XOR	exclusive OR
XSD	XML Schema Definition
XSL	Extensible Style Sheet Language
XSLT	Extend ble Style Sheet Language Transformation
XSS	cross-site scripting
ZSK	zone signing key

B. FUNCTIONAL, ARCHITECTURAL AND PERFORMANCE REQUIREMENTS

1.1 Legal and Regulatory Requirements to be met by the Information System

1.1.1 The Information System MUST comply with the following laws and regulations:

1.1.1.1 Digital Security Act 2016

1.1.1.2 Policies, Guidelines, and Standards

- Government of Bangladesh Information Security Manual 2016
- ICT Policy 2009 amended in 2015
- Guideline on ICT Security For Banks and Non-Bank Financial Institutions 2015
- Information Security Policy Guideline 2014
- National Cyber Security Strategy 2014
- Cyber Security Policy 2010
- ISO 27001:2013

1.2 Business Function Requirements to be met by the Information System

1.2.1 The Information System MUST support the following business functions:

1.2.1.1 The general business requirement is to acquire and maintain cyber defense skills development capabilities within Government of Bangladesh. Acquired capabilities will train IT-related personnel to protect digital assets in their organisations at cyber space and deal with cyber security incidents when they occur. Cyber defense skills development service will also contribute to cyber security awareness activities within the Government of Bangladesh, and foster cybersecurity incident response skills.

1.2.1.2 Cyber Security Simulation Lab Platform should be a ready to use platform for simulating and learning of real world cyber security experience for trainee stuffs. It will be a simulated testing environment that will simulate the network and applications of a standard enterprise customer's network. This simulated lab environment should be a complete network, server and application infrastructure environment. The application and network infrastructure zone will represent a typical internal IT network environment, simulating an Internet border gateway (gateway-block), data center and application services (server block), and local and remote user access infrastructure (user block).

1.2.1.3 The proposed Cyber Attack Simulation would work as a service-based organization. It has to organize standardized cyber defense skills development through cyber security exercises named "Cyber Attack Simulation" on a regular basis as well as on special request. It has to ensure basic and advance level cyber security skills development capabilities during its whole lifecycle. The proposed Cyber Attack Simulation Center has to be a platform to learn cyber security on real world scenarios. Think of a flight simulator where pilots learn how to handle complex systems in different flight situations. The Cyber Attack Simulation will be a similar environment for cyber security staff. Cyber Attack Simulation will be a sandpit environment that will simulate the network and applications of a typical enterprise. But the solutions will not just focus on technology; it will look into the people, skills, processes, and data and obviously at all things that are connected to the internet. The proposed Cyber Attack Simulation Services at Bangladesh Computer Council will be built upon the following components:

- ❖ It would be operations-driven and able to bring together people, process, and technology in responding to threat scenarios
- ❖ It would leverage threat focused, visibility driven, and platform based security tools
- ❖ It would be capable of simulating various attack scenarios including the latest attack and threat scenarios
- ❖ It would use a virtual environment that can be accessed remotely from any place in the world

The deployed solution should ensure attack zone and defense zone which will be separated through an internet border gateway so that cyber-attack simulation can be done from an external environment and not from within the organization. The solution is meant to test real life cyber war exercises and accordingly identify and define incident response practices, thereby, the proposal should include necessary subscription services to update the simulation environment with threat intelligence once every year for a minimum of 3 years.

1.2.1.4 Expansion of internet infrastructure worldwide results in raising count of cyber incidents, including in government organizations. It is due to interconnectivity, government organizations continuously developing IT assets whose are accessible to its clients as well as for malicious actors. These assets face cyber threats every day and some of them are being affected. BGD e-GOV CIRT (the unit which is responsible for handling cyber incidents within the Government of Bangladesh) statistic shows that every day at least one publicly available asset (like a webpage) is being affected. This comes by having limited visibility and in reality it means that the issue is many times bigger.

Besides reactivity to deal with cyber security incidents occurred and BGD e-GOV proactive services like cyber security awareness, the Government of Bangladesh needs a platform where IT-related personnel may practically and in safe environment develop their cyber security defence skills. It will result in proactive activities to protect current vulnerable assets and avoidance of cyber security incidents in the future.

1.2.1.5 Objectives of the Cyber Attack Simulation Solution

The objectives of the Cyber Attack Simulation will be the following:

a) **Simulate Various Attack Scenarios;** To be used as a simulator of large-scale virtual networks (IT, SCADA, tactical communications, etc.) and attacks based on previous real-world incidents, including SCADA attack scenarios.

b) **Provide Cyber Warrior Training;** to be used as a scaled model of the real world with standardized curriculum for the real-world exercises needed to build skills and hone cyber warrior instincts. Using self-paced training and hands-on Cyber Attack Simulation exercises, personnel can be transformed into cyber warriors. Provide a training ground to exercise the operational scenarios to understand and defend cyber attacks.

c) **Serve as a Validation Tool;** to be used as a validation tool where organizations can evaluate their security infrastructure and find out the exact equipments that fit their cyber security needs.

d) **Test Application Performance;** to be used as a tool to test application performance over the network.

e) **Asses Skills and Knowledge;** to be used for assessment team's skills and knowledge in defending cyber attacks.

f) **Cyber War Games;** to be used as a platform for red and blue teams to test their offensive and defensive skills and strategies.

1.2.1.6 Other Goals of the Cyber Attack Simulation Solution

a) **Standardize** – A comprehensive test solution and test plan with appropriate test cases, which test and verify key aspects of a Cyber Attack Simulation
b) **Efficiency and Repeatability** – A solution which provides timely testing with minimal engineering time on a per incident basis
c) **Valuable Reporting and Analysis** – A solution which enables a customer to quickly gauge performance, quantify results, and actionable information

1.3 Architectural Requirements to be met by the Information System

1.3.1 The Cyber Attack Simulation Solution MUST be supplied and configured to implement the following architecture.

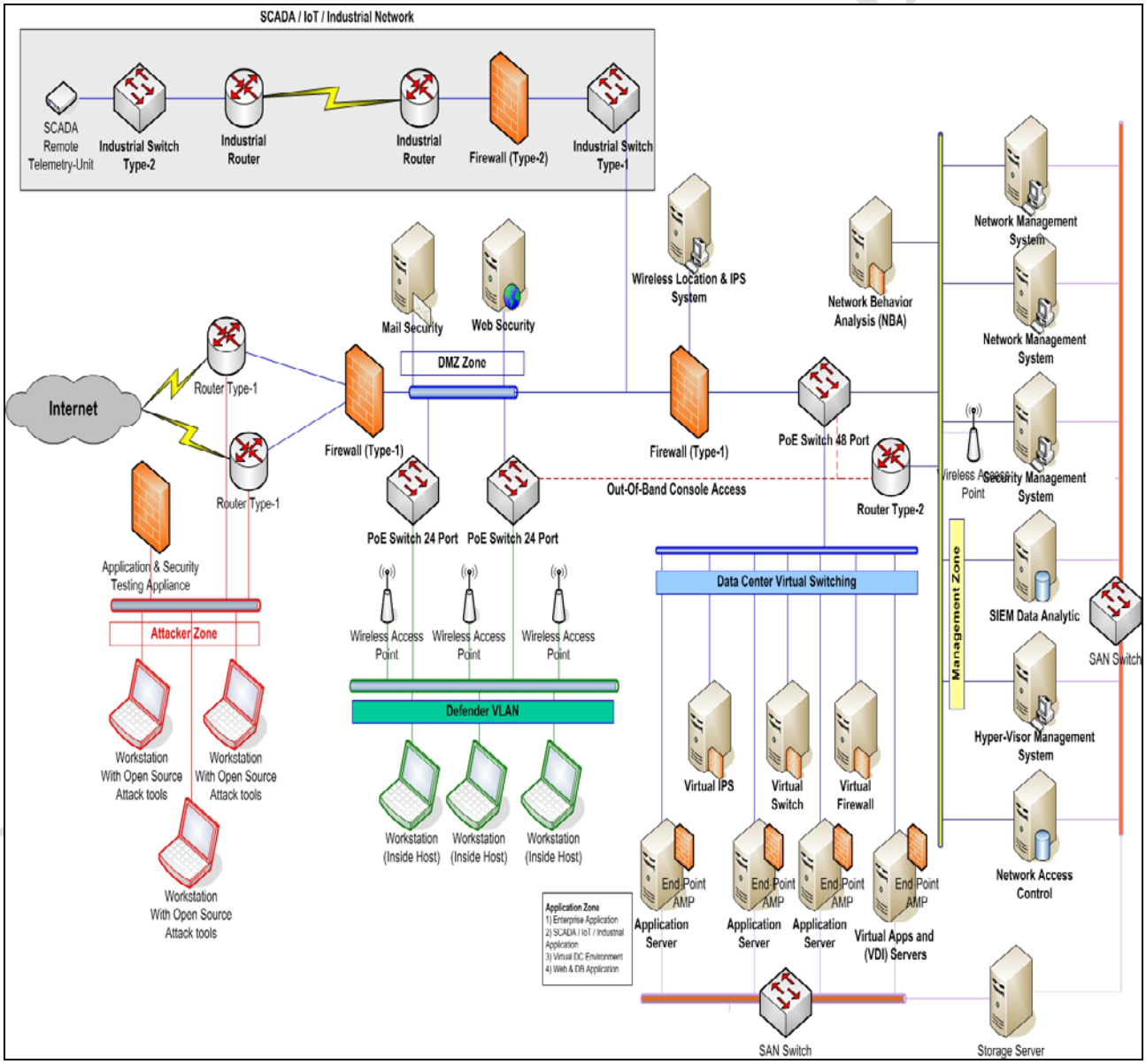

Figure – 1: Cyber Attack Simulation Network Architecture

1.3.2 Cyber Attack Simulation Security Simulation Laboratory Capabilities (The bidder must comply 100% with the requirements stipulated hereinafter)

Infrastructure	Attack	Visibility and Control
• Wired, Wireless and Remote Access • Network and Routing • Client Simulator • Server Simulator • Application Simulator • Traffic Generation	• Day 0 Attack/New Threats • DDoS • Network Reconnaissance • Application Attacks • Data Loss • Computer Malware • Mobile Device Malware • Wireless Attacks • Evasion techniques • Botnet Simulation • Open Source attack Tools • Virtual Network Attacks	• Global Threat Intelligence (Cloud) • Firewall and IDS/IPS • Signature based detection • Behavior based detection • Data Loss prevention • Web and Mail Security • Application visibility and Control • Wireless Security • Identity and Access management • Event Correlation • Packet capture and Analysis • Virtual Network Security • Network Group Security • Software Defined Network

- Full device installation and configurations inside Cyber Attack Simulation environment, including:
    a. Next Generation Firewall
        - Provides control and monitoring of incoming and outgoing network traffic based on a defined set of rules (e.g. access control, advanced threat and breach detection etc.) for both virtual and physical infrastructure
    b. IPS (Intrusion Prevention System)
        - Provides application visibility and control, threat protection, real-time contextual awareness, intelligent security automation with optional subscription licenses of Advanced Malware Protection (AMP) for both virtual and physical infrastructure
    c. Network Net Flow and Behaviour Security
        - Detect anomalous traffic and behaviours, including zero-day malware, distributed denial-of-service (DDoS) attacks, insider threats, and advanced persistent threats (APTs) on both virtual and physical infrastructure
    d. Web Security
        - Provide proxy service that combines traditional URL filtering with dynamic content analysis in real time to mitigate compliance, liability, and productivity risk for corporate users and applications.
    e. Email Security
        - Provides preventive and reactive measures of various viruses, spam, ransomware, phishing (fraud), spoofing, data leakage and advanced malware attack to strengthen email security.
    f. Wireless Security
        - Make use of the wireless infrastructure to detect, locate, mitigate, and contain wired and wireless rogues and threats at Layers 1 and 2.
    g. Network Access Control and Policy
        - Allow to see and control users and devices connecting to the corporate network. It does all this from a central location.
    h. Threat Generator
        - Simulating real-world legitimate traffic, distributed denial of service (DDoS), exploits, malware, and intrusions
    i. SIEM and Data Analytics System
        - Provides a single pane of glass interface into correlated security data.

Following list is of the attack cases classified by the detection technologies, implementation techniques or using scenario during the Cyber Attack Simulation Workshop. The delivered attack cases vary from fundamental to complex/ mixed /sophisticated /APT, could be generated by tool or manual built to fulfill the training requirements during the Cyber Attack Simulation Workshop.

a) Cyber Attack Simulation Practice Lab. The following is the complex attack cases that require the use of more than 2 defense systems to detect them. Sometimes, all defense tools are used altogether with correlation analysis to discover the root cause. The Practice Lab is more or less simple case for learning/practicing purpose.
    1. 1st round of the practice lab
    2. 2nd round of the practice lab

a) Next Generation Firewall and IPS. These attack cases are detected mainly by FW and IPS systems using the signature based technology. Threat Generator system is used to generate the attacks
    1. Threat detection with firewall
    2. Malware detection and analysis
    3. "SQL slammer" worm detection
    4. Application awareness and visibility
    5. Packet captures for attack investigation

b) Web Security. Related to Web attacks that are built manually or by using the Threat Generator.
    1. Reputation based filtering
    2. Malware filtering
    3. Data leak prevention
    4. Web usage policy

c) Email Security. Related to email attacks that are built manually or by using the Threat Generator.
    1. Email spam
    2. Phishing attack
    3. Data Leak Prevention
    4. Viral email outbreak
    5. Keyword based scan

d) Network Behaviour Based Detection for signature based detection system attack. The Lab Intelligence Center provides the threat intelligent for attack identification.
    1. Network behaviour reputation
    2. Reconnaissance
    3. Data loss prevention
    4. Malware detection
    5. External attacks

e) Network Access Control and Policy. Attack based on the identity spoofing technique. These attacks are built manually.
    1. Device spoofing
    2. Shared credential policy violation
    3. User location correlation

f) Wireless Security. Attack from wireless devices. These attacks are built manually
    1. Interference Detection
    2. Rogue AP Detection
    3. Wireless Attack Detection
    4. Network Group tag access control
    5. Tag based guest access

g) Virtual Security. Attacks in virtual environment. All are built manually.
   1. Inter-VDC attacks
   2. Intra-VDC attacks
   3. Data leakage detection

h) DDoS. Different DDoS attacks built with Threat Generator.
   1. Volumetric attacks
   2. Reflection attacks
   3. State exhaustion
   4. Application layer attacks
   5. Advanced DDoS attacks

i) Hacking and C&C module. About Command and Control setup and technique to detect the attacks via the identification of connection to CC server. All attack cases built manually.
   1. Command & Control through weaponized Word document
   2. Command & Control through server vulnerability

j) Bonus Labs
   1. Malware APT Attack
   2. Email end user education APT Attack
   3. Application Visibility Practice Lab
   4. Stage Attack APT
   5. Multi-Vector APT Attack

k) Cyber Attack Simulation Mixed Attacks. The Mixed attack is attack with at least 2 activities. Some attack cases are phased attack based on the kill chain with the phases 1, 2, 3 and so on.
   1. 1st round of mixed attacks
   2. 2nd round of mixed attacks
   3. 3rd round of mixed attacks

l) Cyber Attack Simulation Security Competitions. The Competition attack is similar to mixed attack with more constrain in time for choosing the best team in the workshop. The restriction on time is needed to simulate the real environment when attack happen in corporate network.
   1. 1st round of competitions case
   2. 2nd round of competitions case
   3. 3rd round of competitions case

1.4 Systems Administration and Management Functions required to be met by the Information System

1.4.1 The Information System MUST provide for the following management, administration, and security features at the overall System level in an integrated fashion.

1.4.1.1 <u>Installation, Configuration and Change Management</u>:

The Successful Bidder should undertake a complete life cycle management approach for providing the required services. This would include:

- Analyze
- Design
- Install
- Configure
- Test
- Implement

All equipments including software should need to be installed in the designated location by BCC. Vendor must install, implement, and integrate all the systems supplied and required for smooth and seamless functioning of the installed systems/equipments. The following requirements must be met by the selected bidder:

- The Systems shall be tested in the staging environment at BCC before installation in the production environment. The winning bidder shall provide documentation to satisfy the purchaser that the selected bidder has tested the functionality, performance based on simulation scenarios and resilience of the various components of the System prior to operational acceptance test.
- The winning bidder shall conduct the tests on the System in the testing and production environments to ensure that the equipments and systems have been installed and setup properly.
- The scope of the system integration tests shall cover integration and interoperability tests on the Systems and on the functional requirements specified in this tender.
- The winning bidder must verify and ensure that all related systems maintain data integrity and can operate in coordination with other systems in the same environment. The winning bidder must ensure that all components are integrated successfully to provide expected results.

Change Management:

Identifying Changes; The first issue in establishing formal change control is delineating a change from a clarification. The selected vendor must ensure that the inventory of what is to be delivered is quickly and concisely bound.

Change Control Procedure; The change control procedure will contain the following key steps:

- BCC will request changes and authorized person from supplier will document and initiate changes.
- BCC and supplier will define the procedures for submitting and evaluating changes in the contract..
- The third is to identify the points where each given deliverable will come under change control. The selected vendor must describe how each of these steps will be accomplished.

Change Control and Planning;

- Even if a change request is turned down, it takes resources to evaluate it. While the evaluation process may consume only a small portion of the project's resources, it tends to take up a large percentage of the time of key resources. The selected vendor must ensure that the resources required for evaluating and implementing changes are included in the project plan.
- If a change request is accepted, it will require resources to complete it. The selected vendor should assume that some of level of change will occur and account for it in the planning process.

1.4.1.2 <u>Operational Monitoring, Diagnostics, and Troubleshooting</u>:

- 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 Attack Simulation infrastructure supplied, installed and commissioned by them under this tender.

- BCC and the successful bidder should agree upon the contractual period and service levels for providing the necessary services.

- All systems, equipments, software and required licenses should be procured, installed, configured, implemented and maintained by the successful bidder during the period of the contract.

1.4.1.3 User Administration and Access Control;

User and Usage Monitoring and Audit Trails: The purchaser wants to ensure that user and usage monitoring and audit trails features are available for all systems and/or equipments that will be installed under this tender. Because at the heart of most devices that provide protection for IT networks is an ability to log events and take actions based on those events.

1.4.1.4 System and Information Security and Security Policies: The successful bidder must follow the recommendations/guidelines/procedures stipulated under ISO 27001:2013 family of standards.

1.4.1.5 Back-up and Disaster-Recovery: The successful bidder must provide detailed procedure and guidelines for back-up and disaster recovery for all systems/equipments that will be installed under this tender.

1.5 Performance Requirements of the Information System

1.5.1 The Information System MUST reach the following performance levels.

1.5.1.1 The decisive performance level that BCC wants to have from the proposed Cyber Attack Simulation is to have the highest level of confidence in the area cyber defense training in a simulated environment through accommodation of current cyber attack scenarios on various types of target equipments , which would facilitate development of highly skilled cyber security workforce capable of ensuring a safe and secure cyber space for the country.

C. SERVICE SPECIFICATIONS – SUPPLY & INSTALL ITEMS

2.1 System Analysis, Design and Customization/Development

2.1.1 The Supplier MUST perform the following Analysis and Design activities using a formal system analysis/development methodology with the following key activities and design deliverables.

2.1.1.1 Detailed Analysis:

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 Attack Simulation platform will be made.

2.1.1.2 Physical Design:

The requirement specifications from the detailed analysis phase must be studied in this phase and then final logical and physical system design will be prepared. In the end of this phase the selected vendor will submit the final design of the proposed Cyber Attack Simulation platform. The final design document must include detailed software and hardware architectures of the proposed Cyber Attack Simulation platform. The design document must be approved by the purchaser.

2.1.1.3 Integrated System:

With inputs from physical design stage, the selected vendor will first implement the Cyber Attack Simulation platform in units, which are integrated in the next phase. The details of integration requirements must be documented and presented to the purchaser for approval along with procedures for testing each and every unit separately and post integration test for the entire system or platform.

2.2 Software Customization / Development

2.2.1 The Supplier MUST perform Software Customization / Development using a formal software development methodology with the following characteristics and/or with the following technologies and/or tools.

2.2.1.1 The selected vendor must provide a document to the purchaser describing the methodology that will be followed by them for implementation of the proposed Cyber Attack Simulation Solution suitable for country requirements.

2.3 System Integration (to other existing systems)

2.3.1 The Supplier MUST perform the following Integration Services:

2.3.1.1 The selected vendor must provide integration services for the Cyber Attack Simulation to receive and analyze data from SIEM system, Firewall, IPS, Routers, Switches, Flow Analyzer, Anti APT system, Email Security Gateway, Network Monitoring System, etc for creating the simulation environment.

2.4 Training and Training Materials

2.4.1 The Supplier MUST provide the following Training Services and Materials.

2.4.1.1 User: Not Applicable

2.4.1.2 Technical: As per the requirements mentioned in this RFB

2.4.1.3 Management: As per the requirements mentioned in this RFB

2.5 Data Conversion and Migration

2.5.1 The Supplier MUST provide services and tools to perform the following Data Conversion and Migration Services: Not Applicable

2.6 Documentation Requirements

2.6.1 The Supplier MUST prepare and provide the following Documentation.

2.6.1.1 End-User Documents: Not Applicable

2.6.1.2 Technical Documents:

- Technical Data Sheet (Software and Hardware)
- Software Technical Manual
- Hardware Technical Manual
- Operational Manual (Entire System)
- Troubleshooting Guide (Software and Hardware)
- Software Customization Manual
- System Administration and Management Guide
- Integration and Interoperability Guide

Note: All technical documents must be in English and must be written in simple and comprehensible manner.

2.7 Requirements of the Supplier's Technical Team

2.7.1 The Supplier MUST maintain a technical team of the following roles and skill levels during the Supply and Installation Activities under the Contract:

2.7.1.1 Team leader (1 person): At least master's degree with minimum 15 years' experience of working in a leadership role in designing and deploying country level information security frameworks and related automation. Have experience in setting up Cyber Attack Simulation technical framework and minimum 3 years' experience of deploying Cyber Attack Simulation in at least two countries. The team leader should have ISACA/EC Council/SANS/CISSP/Equivalent Certification.

2.7.1.2 Project governance and management specialist (1 person): At least master's degree with minimum 10 years' experience in governance and management of information security projects in at least two countries. The incumbent must have CGEIT and Prince2 or alternative IT governance and project management certificates.

2.7.1.3 Senior Expert in Cyber Attack Simulation operations (1 person): At least master's degree with minimum 3 years' experience in structuring and setting up and running professional Cyber Attack Simulation . The incumbent must have experience in providing Cyber Attack Simulation specific training, and running Cyber Attack Simulation operations. The person must have Cyber Security Analysis experience.

2.7.1.4 Expert in information security analysis (1 person): Must have minimum 5 years' experience in information security operations and most importantly as a security analyst in a Cyber Attack Simulation setup. The person must also have expertise in technical investigation of cyber security attacks and breaches.

2.7.1.5 Expert in information security delivery (1 person): Must be serving as a senior information security manager (for at least of two years), preferably CISO and supervising information security program. The person must be certified in Information Security Management (CISM or alternative). The incumbent must have experience of setting up Cyber Attack Simulation and minimum 6 years' experience in information security delivery.

2.7.1.6 Local cyber security expert (1 person): Must have experience of operations of dedicated cyber security team in a large organization, experience of working in a Cyber Attack Simulation setup is a plus. Current experience of working with Firewall, IPS, SIEM, and NMS in a SOC environment is required. The incumbent must be a resident Bangladeshi National with minimum 8 years' experience in cyber security.

D. TECHNOLOGY SPECIFICATIONS – SUPPLY & INSTALL ITEMS

3.0 General Technical Requirements

3.0.1 Language Support: All information technologies must provide support for the English language.

3.0.2 Electrical Power: All active (powered) equipment must operate on **voltage range and frequency range [**220v +/- 20v], [50Hz +/- 2Hz] respectively. All active equipment must include power plugs standard in Bangladesh.

3.0.3 Environmental: Unless otherwise specified, all equipment must operate in environments of **temperature:** 10-30 degrees centigrade**, humidity:** 20-80 percent relative humidity **and dust condition:** 0-40 grams per cubic meter of dust.

3.0.4 Safety:

3.0.4.1 Unless otherwise specified, all equipment must operate at noise levels no greater than 55 decibels.

3.0.4.2 All electronic equipment that emits electromagnetic energy must be certified as meeting US FCC class B or END 55022 and END 50082-1, or equivalent, emission standards.

3.1 Technical Requirement

3.1.1 Technical Specifications of following items are covered:

Detailed Technical Specifications and Requirements for all items are provided in section 3.1.3.

3.1.2 Work plan and Design of Cyber Attack Simulation

The implementation part of assignment mentioned in this invitation for bids must be completed within 1 calendar year from the date of signing the contract, and implementation timeline is 365 Calendar days from the date of signing of contract. Total project duration is 24 months. Detailed technical designs and relevant documentation must be provided including physical, logical and service oriented layout designs, test case designs, etc. Roles and responsibilities of all stakeholders regarding the activities and services must be provided in details with clear separation of duties.

Implementation Schedule

SL. #	Task Description	Duration (T +No. of Days)
1	Signing of Contract	T = Date of Contract Signing
2	Detail design of the implementation of the Cyber Attack Simulation	T1 = T + 60
3	Deliver of Hardware and Software Platforms	T1
4	Training Designing and Development of Training and Operation Manuals	T1
4	Cyber Attack Simulation Installation, Configuration and Integration Services	T2= T1 + 15
5	Custom Training on Creation of Test Cases	T3= T2 + 15
SL. #	**Task Description**	**Duration (T +No. of Days)**

SL. #	Task Description	Duration (T +No. of Days)
6	Advanced Cyber Attack Simulation Essentials Training	T4 =T3 + 15
7	On Premises Support	T5= T4 + 60
8	Remote Support	T6 = T5 + 365
9	Updates and Maintenance of Software Components	Three (3) years from the date of go-live of the Cyber Attack Simulation
10	Warranty	Three (3) for Years from the date of go-live of the Cyber Attack Simulation .

3.1.3 Detailed Technical Specifications and Requirements

Item-1: Detailed design of the implementation of the Cyber Attack Simulation				
SL. #.	**Product Names/Items**	**Description of requirements**	**UoM**	**QTY**
1	**General**	Detail design of the implementation the Cyber Attack Simulation : 1. The Cyber Attack Simulation must be able to accommodate at least twelve (12) trainees in a single training session 2. Detail technical and functional architecture of the deployable technologies, their relationships 3. Services model and description 4. Implementation project plan 5. Resources required to establish and run the Center **Note**: Document should include designs for all items of the project.	Set	1
Item-2: Applications and Security Testing Appliance				
SL. #.	**Product Names/Items**	**Technical Specifications**	**UoM**	**QTY**
2	Enterprise Scale Applications and Security Testing with Application and Threat Intelligence (ATI)	PerfectStorm ONE Fusion, 1 Gig, 8-PORT SFP APPLIANCE (PS1GE8NG); along with BreakingPoint Application & Threat Intelligence (ATI) (909-0856) Eight (8) 1GE SFP optical transceivers/cable assemblies	Set	1
Item-3: Application and Threat Intelligence Program				
SL. #.	**Product Names/Items**	**Technical Specifications**	**UoM**	**QTY**
3	Application and Threat Intelligence Program	Application and Threat Intelligence Program for three (3) years to be bundled with item-2.	Set	1
Item-4: Application Server				
SL. #.	**Product Names/Items**	**Technical Specifications**	**UoM**	**QTY**
4	Application Controller	(AppServ-01) 1U Multi-User Application Controller, Includes Windows 2012 Server Standard Edition (64 bit) with 10 user Terminal Server License; Dual 2.1 GHz 8 Core Processors, 64GB RAM, 480 GB Enterprise Value 6G SSD SATA hard-drive, DVD ROM/Virtual DVD, 1.2 TB 12G SAS 10K RPM hard-drive, 4 x 10/100/1000-Base-T Port, Dual AC Power Supply.	Set	2
Item-5: Interfaces				
SL. #.	**Product Names/Items**	**Technical Specifications**	**UoM**	**QTY**
5	Different Interfaces for enterprise scale Security Testing and Application and Threat Intelligence Appliances	1000BASE-SX Dual-Rate pluggable optical transceiver for 1 Gigabit Ethernet LAN/WAN load modules with pluggable SFP interface, 850nm. Compatible with all 1 Gigabit Ethernet, PerfectStorm modules and appliances. Note: Multi-mode fiber LC-LC, 3 meter cable must be included.	Set	8
Item-6: Analog Platform				
SL. #.	**Product Names/Items**	**Technical Specifications**	**UoM**	**QTY**
6	Analog Platform	Analog Devices Platform Bundle	Set	1
Item-7: Server				
SL. #.	**Product Names/Items**	**Technical Specifications**	**UoM**	**QTY**

		Backend and end-user infrastructure for cyber defense exercises development, storing, running, maintaining, and backup		
7	**Server**		Set	5
	Model and Brand	To be mentioned		
	Rack type	Rack mountable, 2U server with dual power supply		
	RAM	At least 768 GB DDR4-2400-MHz, extendable at least to 1.5TB		
	Internal storage	At least 8 x 960GB Enterprise Grade 6G SATA SSD for each server, at least 12G SAS RAID with 4GB Cache RAID 60 enabled, 24 HDD slots		
	CPU	2 x Intel E5-2667 v4 3.20 GHz 8 Core Processor or higher model		
	Virtualization support	HyperV, VMware and Xen support		
	LAN	At least 6 interfaces for 10/100/1000 Base-TX, full-duplex, at least 2 interface 10Gbps ports, 2 interfaces for 8G Fiber Channel HBA ports		
	Specific warranty for server hardware	3 years full warranty. Faulty spare part delivery in 2 working days, on-site.		
	Deployment	Including delivery service, installation on site, integrity tests, and connecting to the backup server		
Item-8: Workstation				
SL. #.	**Product Names/Items**	**Technical Specifications**	**UoM**	**QTY**
8	**Workstations**	Frontend infrastructure to be used by trainees during cyber defense exercises. Must consist of hardware, with at least the following requirements:	Set	15
	Brand and Model	To be mentioned		
	Type	Desktop type, might be integrated with a monitor		
	RAM	At least 32 GB at least DDR 2133 MHz		
	HDD	At least 200 GB SSD		
	CPU	At least 7000 or more points according to “Passmark CPU Mark“ found at http://www.cpubenchmark.net/cpu_list.php		
	Motherboard	At least Intel X99 or equivalent chipset		
	GPU	At least - 2 GB GDDR5, DVI, HDMI		
	Monitor	At least 1920x1080 pixels, display size at least 21,5” (16:9) with DVI, HDMI, including cable		
	Keyboard and mouse	Standard, wired, mouse with 3 keys and wheel.		
	Specific warranty for workstation hardware	Three years full warranty. Faulty spare part delivery in 2 working days, onsite.		
	Related services	Including delivery service, installation on site and connection to the centralized hardware infrastructure		
	Operating system for workstations	Windows 10 Pro or alternative		
Item-9: Whiteboard				
SL. #.	**Product Names/Items**	**Technical Specifications**	**UoM**	**QTY**
9	**Wall Whiteboards**	Must fit at least the following requirements: 2 meters length, 1 meter high, white, with wall hangers and small shelf at the bottom to keep small equipment like markers, to be deployed at 3 different classrooms.	Set	3
	Brand Name:	To be mentioned		
	Model Name:	To be mentioned		

Item-10: Monitor				
SL. #.	**Product Names/Items**	**Technical Specifications**	**UoM**	**QTY**
10	**Monitor**	Screen size: 42-inch Aspect ratio: 21:9 | Resolution: 3440 x 1440 Brightness: 340 cd/m2 Response time: 14ms Viewing angle: 172/178 Contrast ratio: 1000:1 Colour support: SRGB 100% Weight: 7.9kg Ports: HDMI and USB	Set	2
	Model Name:	To be mentioned		
	Brand Name:	To be mentioned		

Item-11: PoE Switch (24 Port)				
SL. #	**Product Names/Items**	**Technical Specifications**	**UoM**	**QTY**
11	Quality	ISO 9001/9002 for manufacturer, FCC Class A/B for quality assurance	Set	2
	Brand	To be mentioned by the bidder		
	Model	To be mentioned by the bidder		
	Environmental	Maintain International Quality Environmental Safety standard		
	Enclosure Type	Rack Mountable with Rack Mounting Kit		
	Part No,	Bidder should submit BOQ of proposed device including the details part numbers. Bidder should submit the required feature & performance compliance document for the proposed solution.		
	Switch Architecture	The Switch should have at least 24 x 1GE 10/100/1000BaseT PoE/PoE+ ports		
		The Switch should have dedicated 2 x 10G modular uplink ports with 2 x 10G Single Mode SFP. All the SFP should be OEM original SFP.		
		The Switch should have at least 430 Watt PoE capacity.		
		The Switch should support Redundant Power Supplies		
		The Switch should be Stackable from Day 1.		
		The Switch Architecture should be able to Stack at least 4 Switches together.		
		The Switch stack should be based on Distributed Forwarding Architecture, where in each stack member forwards its own information on network.		
		The Switch Stack Architecture should have centralized control and Management plane with Active Switch and all the information should be Synchronized with Standby Switch.		

		The Switch should support Stateful Switchover (SSO) when switching over from Active to Standby switch in a Stack.		
		The Switch Stack Architecture should be Plug & Play for attaching or removing any switch from the stack without any downtime.		
		The Switch should be based on a Modular OS Architecture capable of hosting applications.		
		The Switch should have RJ45 & Mini USB Console Ports for Management		
		The Switch should have USB 2.0 for OS Management (uploading, downloading & booting of OS and Configuration)		
		The Switch should have at least 1x 10/100/1000 dedicated Ethernet Management Port		
		The Switch should have at least 3 fans and in case of failure of any one of those the other fans should automatically speed up. Fans should be field replaceable.		
		The Switch should have power savings mechanism wherein it should reduce the power consumption on ports not being used.		
		The switch should be Rack Mountable and should not take space more than 1RU.		
	Wireless Controller	The switch should support at least 100 wireless access points in single switch or cluster.		
		Bidder must propose 1 wireless access point license for each switch.		
	Switch Performance	The Switch should have at least 88Gbps switching bandwidth.		
		The switch should have at least 65 Mpps of forwarding rate.		
		The Switch should have at least 200Gbps Unidirectional or 400Gbps Spatial Reuse Stack Bandwidth.		
		The Switch should support at least 31000 MAC Addresses		
		The Switch should support at least 23000 IPv4 routes		
		The Switch should support at least 4000 VLAN ID's & 1000 Switch Virtual Interface (SVI)		
		The Switch support 9198 bytes of Jumbo Frames		
	Layer 3 Features	The switch should support routing protocols such OSPF, BGPv4, IS-ISv4.		
		The Switch should support IPv6 Routing capable protocols such as OSPFv3 in hardware.		
		The Switch should support Policy Based Routing (PBR) or similar technology		

		The Switch should support IP Multicast and PIM, PIM Sparse Mode, PIM Dense Mode, PIM Sparse-dense Mode & Source-Specific Multicast for Wired and Wireless Clients.		
		The switch should support basic IP Unicast routing protocols (static, RIPv1 & RIPv2) should be supported.		
		The switch should support Policy Based Routing or similar technology		
	Layer 2 Features	The Switch should be able to discover (on both IPv4 & IPv6 Network) the neighboring device giving the details about the platform, IP Address, Link connected through etc, thus helping in troubleshooting connectivity problems.		
		The switch should support Detection of Unidirectional Links (in case of fiber cut) and to disable them to avoid problems such as spanning-tree loops.		
		The switch should support centralized VLAN Management; VLANs created on the core switch should be propagated automatically.		
		The switch should support 802.1d, 802.1s, 802.1w Spanning-Tree & its Enhancement for fast convergence.		
		The switch should support 802.1q VLAN encapsulation.		
		The switch should support 802.3ad (LACP) to combine multiple network links for increasing throughput and providing redundancy.		
	Network Security Features	The switch should have Port security to secure the access to an access or trunk port based on MAC address to limit the number of learned MAC addresses to deny MAC address flooding.		
		The switch should support DHCP snooping to prevent malicious users from spoofing a DHCP server and sending out rouge addresses.		
		The switch should support Dynamic ARP inspection (DAI) to ensure user integrity by preventing malicious users from exploiting the insecure nature of ARP.		
		The switch should support IP source guard to prevent a malicious user from spoofing or taking over another user's IP address by creating a binding table between the client's IP and MAC address, port, and VLAN.		
		The switch should support Unicast Reverse Path Forwarding (RPF) feature to mitigate problems caused by the introduction of malformed or forged (spoofed) IP source addresses into a network by discarding IP packets that lack a verifiable IP source address.		
		The switch should support Bidirectional data support on the SPAN port to allow the intrusion detection system (IDS) to take action when an intruder is detected.		

		The switch should support flexible & multiple authentication mechanism, including 802.1X, MAC authentication bypass, and web authentication using a single, consistent configuration.		
		The switch should support RADIUS change of authorization and downloadable Access List for comprehensive policy management capabilities.		
		The switch should support Private VLANs to restrict traffic between hosts in a common segment by segregating traffic at Layer 2, turning a broadcast segment into a non broadcast multi access like segment to provide security & isolation between switch ports, which helps ensure that users cannot snoop on other users' traffic.		
		The switch should support Multi domain authentication to allow an IP phone and a PC to authenticate on the same switch port while placing them on appropriate voice and data VLAN.		
		The switch should support MAC address notification to allow administrators to be notified of users added to or removed from the network.		
		The switch should support IGMP filtering to provide multicast authentication by filtering out nonsubscribers and limits the number of concurrent multicast streams available per port.		
		The switch should support VLAN ACLs on all VLANs prevent unauthorized data flows from being bridged within VLANs.		
		The switch should support IPv6 ACLs that can be applied to filter IPv6 traffic.		
		The switch should support Port-based ACLs for Layer 2 interfaces to allow security policies to be applied on individual switch ports.		
		The switch should support Secure Shell (SSH) Protocol, Kerberos, and Simple Network Management Protocol Version 3 (SNMPv3) to provide network security by encrypting administrator traffic during Telnet and SNMP sessions.		
		The switch should support TACACS/RADIUS authentication to facilitate centralized control of the switch and restricts unauthorized users from altering the configuration.		
		The switch should support Multilevel security on console access to prevent unauthorized users from altering the switch configuration.		
		The switch should support Bridge protocol data unit (BPDU) Guard to shut down Spanning Tree PortFast-enabled interfaces when BPDUs are received to avoid accidental topology loops.		

		The switch should support Spanning Tree Root Guard to prevent edge devices not in the network administrator's control from becoming Spanning Tree Protocol root nodes.		
		The Switch should support IPv6 RA Guard, DHCPv6 guard, IPv6 Snooping to prevent any Man-in-middle attack.		
		The Switch should support Dynamic VLAN, Downloadable ACLs, Multi-Auth VLAN Assignment, and MAC Based Filtering & Web Authentication security mechanism.		
	Quality of Service (QoS) & Control	The Switch should support Advanced Modular QoS Policies		
		The Switch should be capable of Queuing, Policing, Shaping and marking Wired and Wireless Traffic based on Class of Service (CoS) or DSCP.		
		The switch should support IP SLA feature set to verify services guarantee based on business-critical IP Applications		
		The switch should support Auto QoS for certain device types and enable egress queue configurations.		
		The switch should support 802.1p CoS and DSCP Field classification using marking and reclassification on a per-packet basis by source and destination IP address, MAC address, or Layer 4 Transmission Control Protocol / User Datagram Protocol (TCP/UDP) port number.		
		The switch should support Shaped round robin (SRR) scheduling to ensure differential prioritization of packet flows by intelligently servicing the ingress queues and egress queues. Weighted tail drop (WTD) to provide congestion avoidance at the ingress and egress queues before a disruption occurs. Strict priority queuing to ensure that the highest priority packets are serviced ahead of all other traffic.		
		The Switch should support Rate limiting based on source and destination IP address, source and destination MAC address, Layer 4 TCP/UDP information, or any combination of these fields, using QoS ACLs (IP ACLs or MAC ACLs), class maps, and policy maps.		
		The Switch should support Eight egress queues per port for wired traffic and four egress queues for wireless to enable differentiated management of different traffic types across the stack for wired traffic.		
		The Switch should support Flexible NetFlow v9 or similar protocol from day 1.		
		The Switch should be capable of enabling flexible flow or similar technology on all ports of the switch for Ingress and Egress Traffic.		
		The Switch should support at least 23000 Flows per switch		
		The Switches when stacked together should be capable to exporting the flow independently / directly to the flow Collector.		

		The Switch should be capable of showing customized reports on OS CLI, based on Top Talkers, Top Destination, Top Protocols etc.		
		The Switch should be capable of monitoring network traffic on Physical, VLAN & WLAN.		
	Standards & Compliance	IEEE 802.1s, IEEE 802.1w, IEEE 802.11, IEEE 802.1D, IEEE 802.1p, IEEE 802.1Q		
		IEEE 802.1x, IEEE 802.1x-Rev		
		IEEE 802.3ad, IEEE 802.3af, IEEE 802.3at, IEEE 802.3x, IEEE 802.3 10BASE-T specification, IEEE 802.3u, IEEE 802.3ab, IEEE 802.3z		
		RMON I and II standards		
		SNMPv1, SNMPv2c, and SNMPv3.		
	Design and Implementation Scope	The OEM will prepare the entire design of the BCC Security LAB keeping in mind the compliance requirements and operational requirements.		
		The OEM Validated Design should take into consideration - scalability, modularity, and resiliency aspects of the Security Lab as well as optimization from space, power and cooling perspective.		
		Respective OEM to also ensure that the final deployment is done basis the OEM specified and validated design standards and best practices.		
	Manufacturer's part number	Bidder should submit BOQ of proposed device/solution including the details part numbers and Manufacturer's Warranty part number.		
		Bidder must submit the required performance document and feature compliance reference document for the proposed device/solution.		
	Warranty	Manufacturer's warranty part number should be mentioned, minimum 3 (Three) years warranty should be provided for this unit from the date of commissioning		
Item-12: PoE Switch (48 Port)				
SL. #	**Product Names/Items**	**Description of requirements**	**Uo M**	**QTY**
12	Quality	ISO 9001/9002 for manufacturer, FCC Class A/B for quality assurance	Set	1
	Brand	To be mentioned by the bidder		
	Model	To be mentioned by the bidder		
	Environmental	Maintain International Quality Environmental Safety standard		
	Enclosure Type	Rack Mountable with Rack Mounting Kit		

	Part No	Bidder should submit BOQ of proposed device including the details part numbers. Bidder should submit the required feature & performance compliance document for the proposed solution.		
	Switch Architecture	The Switch should have at least 48 x 1GE 10/100/1000BaseT PoE/POE+ ports		
		The Switch should have dedicated 2 x 10G modular uplink ports with 2 x 10G Single-Mode SFP. All the SFP should be OEM original SFP.		
		The Switch should have at least 430 Watt PoE capacity.		
		The Switch should have Redundant Power Supplies from day 1.		
		The Switch should be Stackable from Day 1.		
		The Switch Architecture should be able to Stack at least 4 Switches together.		
		The Switch stack should be based on Distributed Forwarding Architecture, where in each stack member forwards its own information on network.		
		The Switch Stack Architecture should have centralized control and Management plane with Active Switch and all the information should be Synchronized with Standby Switch.		
		The Switch should support Stateful Switchover (SSO) when switching over from Active to Standby switch in a Stack.		
		The Switch Stack Architecture should be Plug & Play for attaching or removing any switch from the stack without any downtime.		
		The Switch should be based on a Modular OS Architecture capable of hosting applications.		
		The Switch should have RJ45 & Mini USB Console Ports for Management		
		The Switch should have USB 2.0 for OS Management (uploading, downloading & booting of OS and Configuration)		
		The Switch should have at least 1x 10/100/1000 dedicated Ethernet Management Port The Switch should have at least 3 fans and in case of failure of any one of those the other fans should automatically speed up. Fans should be field replaceable.		
		The Switch should have power savings mechanism wherein it should reduce the power consumption on ports not being used.		
		The switch should be Rack Mountable and should not take space more than 1RU.		

	Wireless Controller	The switch should support at least 100 wireless access points in single switch or cluster.		
		Bidder must propose 1 wireless access point license for each switch.		
	Switch Performance	The Switch should have at least 166 Gbps switching bandwidth.		
		The switch should have at least 125 Mpps of forwarding rate.		
		The Switch should have at least 200Gbps Unidirectional or 400Gbps Spatial Reuse Stack Bandwidth.		
		The Switch should support at least 31000 MAC Addresses		
		The Switch should support at least 23000 IPv4 routes		
		The Switch should support at least 4000 VLAN ID's & 1000 Switch Virtual Interface (SVI)		
		The Switch support 9198 bytes of Jumbo Frames		
	Layer 3 Features	The switch should support routing protocols such OSPF, BGPv4, IS-ISv4.		
		The Switch should support IPv6 Routing capable protocols such as OSPFv3 in hardware.		
		The Switch should support Policy Based Routing (PBR) or similar technology		
		The Switch should support IP Multicast and PIM, PIM Sparse Mode, PIM Dense Mode, PIM Sparse-dense Mode & Source-Specific Multicast for Wired and Wireless Clients.		
		The switch should support basic IP Unicast routing protocols (static, RIPv1 & RIPv2) should be supported.		
		The switch should support Policy Based Routing or similar technology		
	Layer 2 Features	The Switch should be able to discover (on both IPv4 & IPv6 Network) the neighboring device giving the details about the platform, IP Address, Link connected through etc, thus helping in troubleshooting connectivity problems.		
		The switch should support Detection of Unidirectional Links (in case of fiber cut) and to disable them to avoid problems such as spanning-tree loops.		
		The switch should support centralized VLAN Management; VLANs created on the core switch should be propagated automatically.		
		The switch should support 802.1d, 802.1s, 802.1w Spanning-Tree & its Enhancement for fast convergence.		
		The switch should support 802.1q VLAN encapsulation.		
		The switch should support 802.3ad (LACP) to combine multiple network links for increasing throughput and providing redundancy.		

		The switch should have Port security to secure the access to an access or trunk port based on MAC address to limit the number of learned MAC addresses to deny MAC address flooding.		
		The switch should support DHCP snooping to prevent malicious users from spoofing a DHCP server and sending out rouge addresses.		
		The switch should support Dynamic ARP inspection (DAI) to ensure user integrity by preventing malicious users from exploiting the insecure nature of ARP.		
		The switch should support IP source guard to prevent a malicious user from spoofing or taking over another user's IP address by creating a binding table between the client's IP and MAC address, port, and VLAN.		
		The switch should support Unicast Reverse Path Forwarding (RPF) feature to mitigate problems caused by the introduction of malformed or forged (spoofed) IP source addresses into a network by discarding IP packets that lack a verifiable IP source address.		
		The switch should support Bidirectional data support on the SPAN port to allow the intrusion detection system (IDS) to take action when an intruder is detected.		
	Network Security Features	The switch should support flexible & multiple authentication mechanism, including 802.1X, MAC authentication bypass, and web authentication using a single, consistent configuration.		
		The switch should support RADIUS change of authorization and downloadable Access List for comprehensive policy management capabilities.		
		The switch should support Private VLANs to restrict traffic between hosts in a common segment by segregating traffic at Layer 2, turning a broadcast segment into a non-broadcast multi access like segment to provide security & isolation between switch ports, which helps ensure that users cannot snoop on other users' traffic.		
		The switch should support Multi domain authentication to allow an IP phone and a PC to authenticate on the same switch port while placing them on appropriate voice and data VLAN.		
		The switch should support MAC address notification to allow administrators to be notified of users added to or removed from the network.		
		The switch should support IGMP filtering to provide multicast authentication by filtering out nonsubscribers and limits the number of concurrent multicast streams available per port.		
		The switch should support VLAN ACLs on all VLANs prevent unauthorized data flows from being bridged within VLANs.		

		The switch should support IPv6 ACLs that can be applied to filter IPv6 traffic.		
		The switch should support Port-based ACLs for Layer 2 interfaces to allow security policies to be applied on individual switch ports.		
		The switch should support Secure Shell (SSH) Protocol, Kerberos, and Simple Network Management Protocol Version 3 (SNMPv3) to provide network security by encrypting administrator traffic during Telnet and SNMP sessions.		
		The switch should support TACACS/RADIUS authentication to facilitate centralized control of the switch and restricts unauthorized users from altering the configuration.		
		The switch should support Multilevel security on console access to prevent unauthorized users from altering the switch configuration.		
		The switch should support Bridge protocol data unit (BPDU) Guard to shut down Spanning Tree PortFast-enabled interfaces when BPDUs are received to avoid accidental topology loops.		
		The switch should support Spanning Tree Root Guard to prevent edge devices not in the network administrator's control from becoming Spanning Tree Protocol root nodes.		
		The Switch should support IPv6 RA Guard, DHCPv6 guard, IPv6 Snooping to prevent any Man-in-middle attack.		
		The Switch should support Dynamic VLAN, Downloadable ACLs, Multi-Auth VLAN Assignment, MAC Based Filtering & Web Authentication security mechanism.		
	Quality of Service (QoS) & Control	The Switch should support Advanced Modular QoS Policies		
		The Switch should be capable of Queuing, Policing, Shaping and marking Wired and Wireless Traffic based on Class of Service (CoS) or DSCP.		
		The switch should support IP SLA feature set to verify services guarantee based on business-critical IP Applications		
		The switch should support Auto QoS for certain device types and enable egress queue configurations.		
		The switch should support 802.1p CoS and DSCP Field classification using marking and reclassification on a per-packet basis by source and destination IP address, MAC address, or Layer 4 Transmission Control Protocol/User Datagram Protocol (TCP/UDP) port number.		
		The switch should support Shaped round robin (SRR) scheduling to ensure differential prioritization of packet flows by intelligently servicing the ingress queues and egress queues. Weighted tail drop (WTD) to provide congestion avoidance at the ingress and egress queues before a disruption occurs. Strict priority queuing to ensure that the highest priority packets are serviced ahead of all other traffic.		

		The Switch should support Rate limiting based on source and destination IP address, source and destination MAC address, Layer 4 TCP/UDP information, or any combination of these fields, using QoS ACLs (IP ACLs or MAC ACLs), class maps, and policy maps.		
		The Switch should support Eight egress queues per port for wired traffic and four egress queues for wireless to enable differentiated management of different traffic types across the stack for wired traffic.		
		The Switch should support Flexible NetFlow v9 or similar protocol from day 1.		
		The Switch should be capable of enabling Flexible Flow or similar protocol on all ports of the switch for Ingress and Egress Traffic.		
		The Switch should support at least 46000 Flows per switch		
		The Switches when stacked together should be capable to exporting the flow independently / directly to the flow Collector.		
		The Switch should be capable of showing customized reports on OS CLI, based on Top Talkers, Top Destination, Top Protocols etc.		
		The Switch should be capable of monitoring network traffic on Physical, VLAN & WLAN.		
	Standards & Compliance	IEEE 802.1s, IEEE 802.1w, IEEE 802.11, IEEE 802.1D, IEEE 802.1p, IEEE 802.1Q		
		IEEE 802.1x, IEEE 802.1x-Rev		
		IEEE 802.3ad, IEEE 802.3af, IEEE 802.3at, IEEE 802.3x, IEEE 802.3 10BASE-T specification, IEEE 802.3u, IEEE 802.3ab, IEEE 802.3z		
		RMON I and II standards		
		SNMPv1, SNMPv2c, and SNMPv3.		
	Design and Implementation Scope	The OEM will prepare the entire design of the BCC Security LAB keeping in mind the compliance requirements and operational requirements.		
		The OEM Validated Design should take into consideration - scalability, modularity, and resiliency aspects of the Security Lab as well as optimization from space, power and cooling perspective.		
		Respective OEM to also ensure that the final deployment is done basis the OEM specified and validated design standards and best practices.		
	Manufacturer's part number	Bidder should submit BOQ of proposed device/solution including the details part numbers and Manufacturer's Warranty part number.		

		Bidder must submit the required performance document and feature compliance reference document for the proposed device/solution.		
	Warranty	Manufacturer's warranty part number should be mentioned, minimum 3 (Three) years warranty should be provided for this unit from the date of commissioning		
Item-13: Router (Type-1)				
SL. #.	**Product Names/Items**	**Description of requirements**	**UoM**	**QTY**
13	**Quality**	ISO 9001/9002 for manufacturer, FCC Class A/B for quality assurance	Set	2
	Brand	To be mentioned by the bidder		
	Model	To be mentioned by the bidder		
	Environmental	Maintain International Quality Environmental Safety standard		
	Enclosure Type	Rack Mountable with Rack Mounting Kit		
	Part No.	Bidder should submit BOQ of proposed device including the details part numbers. Bidder should submit the required feature & performance compliance document for the proposed solution.		
	Router Processor Type	High-performance multi-core processors		
		Must have Separate control plane, data plane and service plane		
	Routing Performance:	IMIX Traffics / Concurrent WAN service Throughput: minimum 1 Gbps		
		Backplane Capacity: minimum 9.5 Gbps		
	DRAM	Min. 8 GB		
	Flash Memory	Min. 8 GB		
	Interfaces	Router should have Min. 4 x 1GE Routing Port with 2 x 1GE Copper ports and 2 x 1GE SFP Port.		
		Router must have 1 x 10GE port from day 1.		
		Management: 1 x console and 1 x Gigabit Ethernet port for device management		
		Serial: 1 x auxiliary port		
		USB: 2 x USB 2.0 Type A port		
	Security Features	Hardware-based cryptography acceleration (IPSec)		
		Should support Layer 7 context-aware / application aware Firewall features		
		Should Dynamic VPN to connect remote VPN devices		

	Interface support	Support Gigabit Ethernet, T1/E1, Channelized E1/T1		
		Support 24-port switch port module as Layer 3 switch		
	Supporting Protocols	IPv4, IPv6, static routes, Routing Information Protocol Versions 1 and 2 (RIP and RIPv2), Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), BGP Router Reflector, Intermediate System-to-Intermediate System (IS-IS), Multicast Internet Group Management Protocol Version 3 (IGMPv3), Protocol Independent Multicast sparse mode (PIM SM), PIM Source Specific Multicast (SSM), Distance Vector Multicast Routing Protocol (DVMRP), IPv4-to-IPv6 Multicast, MPLS, Layer 2 and Layer 3 VPN, IP sec, Layer 2 Tunneling Protocol Version 3 (L2TPv3), Bidirectional Forwarding Detection (BFD), IEEE802.1ag, and IEEE802.3ah		
	Encapsulations	Generic routing encapsulation (GRE), Ethernet, 802.1q VLAN, Point-to-Point Protocol, Multilink Point-to-Point Protocol, High-Level Data Link Control (HDLC), Serial (RS-232, RS-449, V.35), and PPP over Ethernet		
	QOS Features	QoS, Class-Based Weighted Fair Queuing, Weighted Random Early Detection, Hierarchical QoS, Policy-Based Routing, Performance Routing and network based application detection mechanism		
	Expansion Slots	Min. 3 Network Interface Module Slots		
	High Availability	Support On-Line Insertion (OIR) for Network Interfaces Modules to reduce downtime during fault/repair/upgrade		
		Support Modular OS on open platform		
		Router should have redundant power supply from day 1.		
	Monitoring	Should have SNMP, RMON, Syslog, NTP, DNS, Telnet and SSH		
		Bidder must propose Management system for all network devices for deployment, inventory, troubleshooting and monitoring.		
		Support application performance monitoring		
		Should have Network Flow Statistic, Service Level assurance feature		
		Support application performance monitoring		
		Should have Network Flow Statistic, Service Level assurance feature		
	Design and Implementation Scope	The OEM will prepare the entire design of the BCC Security LAB keeping in mind the compliance requirements and operational requirements.		
		The OEM Validated Design should take into consideration - scalability, modularity, and resiliency aspects of the Security Lab as well as optimization from space, power and cooling perspective.		

		Respective OEM to also ensure that the final deployment is done basis the OEM specified and validated design standards and best practices.		
	Manufacturer's part number	Bidder should submit BOQ of proposed device/solution including the details part numbers and Manufacturer's Warranty part number.		
		Bidder must submit the required performance document and feature compliance reference document for the proposed device/solution.		
	Warranty	Manufacturer's warranty part number should be mentioned, minimum 3 (Three) years warranty should be provided for this unit from the date of commissioning		

Item-14: Router (Type-2)				
SL. #	**Product Names/Items**	**Description of requirements**	**UoM**	**QTY**
14	**Quality**	ISO 9001/9002 for manufacturer, FCC Class A/B for quality assurance	Set	1
	Brand	To be mentioned by the bidder		
	Model	To be mentioned by the bidder		
	Enclosure Type	Rack-mountable Modular Chassis		
	Environmental	Maintain International Quality Environmental Safety standard		
	Part No	Bidder should submit BOQ of proposed device including the details part numbers. Bidder should submit the required feature & performance compliance document for the proposed solution.		
	Architecture	Should be chassis based & modular architecture for scalability and should be a single box configuration for ease of management.		
		Should have hardware based IPSEC VPN (3DES/AES) Encryption card. Should support IPSEC VPN, Firewall features.		
		Router should be quoted with AC power supply.		
		Should have redundant power supply to connect alternate power source		
	DRAM	Min. 512 MB		
	Flash Memory	Min. 256 MB		
	Interfaces Requirements	Min. 2 x 10/100/1000Base-T Routing Port		
		Min 16 x Asynchronous EIA-232 ports		
		Management: 1 x console		
		Serial: 1 x auxiliary - RJ-45 port		
		USB: 1 x USB 2.0 Type A		
	Expansion Slots	Min. 3 WAN Interface Slots for future interface expansion		
	Security	Hardware-based cryptography acceleration		
		Should support SUITE-B VPN Encryption mechanism		
		Should have Dynamic VPN to connect remote VPN devices		
		Should support Stateful Firewall		

		Should support Granular security policies for per-user, per-interface, or per-sub-interface security policies.		
		Should support IPsec Stateful Failover and VRF-aware firewall		
	Data Link Protocol	Ethernet, Fast Ethernet, Gigabit Ethernet.		
	Interface support	4G 800/900/1800/ 2100/2600 MHz, 900/1900/2100 MHz UMTS/HSPA bands		
		3.7G HSPA+ with SMS/GPS		
		T1/E1, Channelized E1/T1, FXS, FXO, VDSL2/ADSL/2/2		
	Protocols	IPv4, IPv6, static routes, Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), BGP Router Reflector, Intermediate System-to-Intermediate System (IS-IS), Multicast Internet Group Management Protocol (IGMPv3), Protocol Independent Multicast sparse mode (PIM SM), PIM Source Specific Multicast (SSM), Distance Vector Multicast Routing Protocol (DVMRP), IPv4-to-IPv6 Multicast, MPLS, Layer 2 and Layer 3 VPN, IPSec, Layer 2 Tunnelling Protocol Version 3 (L2TPv3), Bidirectional Forwarding Detection, IEEE802.1ag, IEEE802.1ad, and IEEE802.3ah		
	Encapsulations	Generic routing encapsulation, Ethernet, 802.1q VLAN, Point-to-Point Protocol, Multilink Point-to-Point Protocol (MLPPP), High-Level Data Link Control (HDLC), Serial (RS-232, RS-449, V.35).		
	QoS Features:	QoS, Class-Based Weighted Fair Queuing, Weighted Random Early Detection, Hierarchical QoS, Policy-Based Routing (PBR) or similar technology, Performance Routing, and Network base Application inspection and treatment.		
		QoS for tunnel interface.		
		Support Modular Quality of Service.		
	Compliant Standards	IEEE 802.3, IEEE 802.1Q, IEEE 802.3af, IEEE 802.3ah, IEEE 802.1ag		
	Monitoring	Should have Telnet, SSH, SNMP, Remote Monitoring (RMON), Syslog, NetFlow / SFlow / Jflow.		
		Should have IPv4 and IPv6 Packet Capture for analysis using an external tool such as Wire shark features for troubleshooting		
		Support management software for automation and auto-configuration		
		Should have capability to monitor events and take informational, corrective, or any desired event action when the monitored events occur or when a threshold is reached		
		Support application performance monitoring		
	Design and Implementation Scope	The OEM will prepare the entire design of the BCC Security LAB keeping in mind the compliance requirements and operational requirements.		
		The OEM Validated Design should take into consideration - scalability, modularity, and resiliency aspects of the Security Lab as well as optimization from space, power and cooling perspective.		
		Respective OEM to also ensure that the final deployment is done basis the OEM specified and validated design standards and best practices.		
	Manufacturer's part number	Bidder should submit BOQ of proposed device/solution including the details part numbers and Manufacturer's Warranty part number.		
		Bidder must submit the required performance document and feature compliance reference document for the proposed device/solution.		

	Warranty	Manufacturer's warranty part number should be mentioned, minimum 3 (Three) years warranty should be provided for this unit from the date of commissioning		
Item-15: Network Management System (NMS)				
SL. #	**Product Names/Items**	**Description of requirements**	**UoM**	**QTY**
15	**Quality**	ISO 9001/9002 for manufacturer, FCC Class A/B for quality assurance	Set	1
	Brand	To be mentioned by the bidder		
	Model	To be mentioned by the bidder		
	Part No	Bidder should submit BOQ of proposed device including the details part numbers. Bidder should submit the required feature & performance compliance document for the proposed solution.		
	Software functional requirements	The Network Management System (NMS) should be Single pane-of-glass solution for complete end-to-end infrastructure management.		
		The Network Management System (NMS) shall be able to manage at least 25 devices and license need to be provided.		
		Network devices like Routers, switches and wireless equipment and other SNMP based devices.		
	Operational features	Support workflows to deployment, and operational tasks		
		Support dashboards and views of relevant information for troubleshooting.		
		Support glance updates of network status through web-client or mail		
		Support Mobile application for smart phone devices to access to view, troubleshoot, and resolve network issues anywhere and anytime		
		Support Integration with knowledge base helps to provide service and support, product updates, best practices, and reports to improve network availability		
		Support service request creation to fix problems		
		Support protocol support helps improve accuracy and completeness, including ping, Link Layer Discovery Protocol (LLDP), Address Resolution Protocol (ARP), Border Gateway Protocol (BGP), Open Shortest Path First (OSPF), and route table lookups.		
		Support grouping and site profiles to manage networks by associating network elements to user groups or to a hierarchical campus/area, building, and floor model.		
		Support network inventory, discovery, manual and bulk import, and software management		
		Support best practices and design configuration templates to enable device and service deployment.		
		Support composite/combined templates to provide flexibility and packaging of individual templates into reusable, purpose-built configurations for consistent and quicker network designs.		
		Support centralized monitoring of wired access networks to maintain robust performance and optimal access connectivity.		

		Support configuration templates for Application Visibility and Control, Firewall, VPN), dynamic multipoint VPN, , access control lists (ACLs) deployment and management		
		Support device-level support for ACLs, Routing Information Protocol (RIP), OSPF, static routes, Ethernet interfaces, and Network Address Translation (NAT) configuration		
		Support reports to use to monitor the system and network health as well as troubleshoot problems.		
		Support AAA for local, RADIUS or Single Sign-on options		
		support Role-based access control		
		Support workflows and tools to help administrators assess service disruptions, receive notices about performance degradation, research resolutions, and take action to remedy non-optimal situations.		
	Server Hardware Requirement	Bidder should propose required Server/hardware to install Monitoring System		
	Design and Implementation Scope	The OEM will prepare the entire design of the BCC Security LAB keeping in mind the compliance requirements and operational requirements.		
		The OEM Validated Design should take into consideration - scalability, modularity, and resiliency aspects of the Security Lab as well as optimization from space, power and cooling perspective.		
		Respective OEM to also ensure that the final deployment is done basis the OEM specified and validated design standards and best practices.		
	Manufacturer's part number	Bidder should submit BOQ of proposed device/solution including the details part numbers and Manufacturer's Warranty part number.		
		Bidder must submit the required performance document and feature compliance reference document for the proposed device/solution.		
	Warranty	Manufacturer's warranty part number should be mentioned, minimum 3 (Three) years warranty should be provided for this unit from the date of commissioning		
	Item – 16: Wireless Location & Wireless Intrusion Prevention System			
SL. #	**Product Names/Items**	**Description of requirements**	**UoM**	**QTY**
16	**Quality**	ISO 9001/9002 for manufacturer, FCC Class A/B for quality assurance	Lot	1
	Brand	To be mentioned by the bidder		
	Model	To be mentioned by the bidder		
	Part No	Bidder should submit BOQ of proposed device including the details part numbers. Bidder should submit the required feature & performance compliance document for the proposed solution.		
	Software functional requirements	The Bidder should propose wireless analytical software including wireless IPS feature for wireless access point and users/end-point.		
		The wireless analytical software including wireless IPS should support at least 180 wireless access points in future if required.		

		The wireless location analytical software with wireless IPS shall be able to manage at least 4 wireless access point and license need to be provided from day 1.		
	Operational features	The software should be capable of below features:		
		Track and locate Wi-Fi devices, interferers, rogues, and RFID tags from single console.		
		Should capable to detect wireless devices presence and receive geo-location or wireless zone-based alerts		
		Should capable for wireless system wide Wi-Fi interference details and correlation information		
		Should capable to provide impact report of wireless interference zone		
		Should support the capability to build custom software/applications to connect users with open location API interface.		
		Should capable to discover and stop security penetration and DoS attacks from wireless connected device		
		Should capable to Monitor, mitigate and report security threats to the wireless network		
		Should capable to Enhance security and regulatory compliance features of WLAN with location intelligence		
	Server Hardware Requirement	Bidder should propose required Server/hardware to install wireless location analytical software with wireless IPS.		
	Design and Implementation Scope	The OEM will prepare the entire design of the BCC Security LAB keeping in mind the compliance requirements and operational requirements.		
		The OEM Validated Design should take into consideration - scalability, modularity, and resiliency aspects of the Security Lab as well as optimization from space, power and cooling perspective.		
		Respective OEM to also ensure that the final deployment is done basis the OEM specified and validated design standards and best practices.		
	Manufacturer's part number	Bidder should submit BOQ of proposed device/solution including the details part numbers and Manufacturer's Warranty part number. Bidder must submit the required performance document and feature compliance reference document for the proposed device/solution.		
	Warranty	Manufacturer's warranty part number should be mentioned, minimum 3 (Three) years warranty should be provided for this unit from the date of commissioning		

Item -17: Virtual Switching Software				
SL. #	**Product Names/Items**	**Technical Specifications**	**UOM**	**QTY**
17	**Quality**	ISO 9001/9002 for manufacturer, FCC Class A/B for quality assurance	Set	4

	Brand	To be mentioned by the bidder		
	Model	To be mentioned by the bidder		
	Part No	Bidder should submit BOQ of proposed device including the details part numbers. Bidder should submit the required feature & performance compliance document for the proposed solution.		
	Software functional requirements	The Bidder should propose data center virtual switching software for virtual machine/hyper-visor and cloud networking.		
		The data center virtual switching software system should support at least 60 Server with virtual hosts, 2000 virtual Ethernet ports, 200 virtual Ethernet ports per physical host, 2000 active VLANs, 2000 port profiles, 30 physical NICs per physical host		
		Bidder must propose the required hardware & software with related resource for Data Center Virtual Switching Software.		
	Operational features	The solution should support Layer 2 switching and advanced networking protocol/functions.		
		Support access control list, AAA, DHCP snooping, Dynamic ARP Inspection, IP Source Guard, IP ACL, MAC ACL, Virtual Security Gateway, Port Security, Unknown Unicast Flood Block, Network Policy etc.		
		Support QoS Classification, QoS Marking, QoS Policing or similar protocol.		
		Support SPAN, Remote SPAN, Netflow/Sflow, Distributed NetFlow v9, SNMP v3, Syslog, SNMP Access Control List		
		Support VxLAN for underlying hardware abstraction/virtualization.		
		Support ISSU, IEEE 802.1Q, Port Channel, Private VLAN, Port Channel LACP, VM/Hyper-Visor Motion, Network vMotion		
		Support Network Load Balancing and virtual path for network services.		
		Support load balancing on virtual Source Port ID, Source MAC Address,		
		Support APIs for Third-Party access/integration, REST API, XML API Support		
	Server Hardware Requirement	Bidder should propose required Server/hardware to install wireless location analytical software with wireless IPS.		
	Design and Implementation Scope	The OEM will prepare the entire design of the BCC Security LAB keeping in mind the compliance requirements and operational requirements.		
		The OEM Validated Design should take into consideration - scalability, modularity, and resiliency aspects of the Security Lab as well as optimization from space, power and cooling perspective.		
		Respective OEM to also ensure that the final deployment is done basis the OEM specified and validated design standards and best practices.		
	Manufacturer's part number	Bidder should submit BOQ of proposed device/solution including the details part numbers and Manufacturer's Warranty part number.		
		Bidder must submit the required performance document and feature compliance reference document for the proposed device/solution.		
	Warranty	Manufacturer's warranty part number should be mentioned, minimum 3 (Three) years warranty should be provided for this unit from the date of commissioning		

Item – 18: Mail Security System				
SL. #	**Product Names/Items**	**Technical Specifications**	**UOM**	**QTY**
18	**Quality**	ISO 9001/9002 for manufacturer, FCC Class A/B for quality assurance	Lot	1
	Brand	To be mentioned by the bidder		
	Model	To be mentioned by the bidder		
	Part No	Bidder should submit BOQ of proposed device including the details part numbers. Bidder should submit the required feature & performance compliance document for the proposed solution.		
	Platform Requirement	The email security system offering should be secure appliance/virtualized based solution		
		The gateway should support a comprehensive email security solution that integrates inbound and outbound defenses against latest email threats such as Graymail detection & Safe unsubscribing, snowshoe spam, viruses, Malicious URL Blocking etc.		
		The solution should support 100 users for anti-spamming, anti-spamming, virus outbreak, data loss prevention and encryption from day one.		
		The solution should support 800 users in future if required.		
		Solution should have false positive efficacy of 1 in 1 million		
		Bidder must propose the required hardware & software with related resource for Mail Security System.		
	Email Security Features	The solution should use their own operating system and MTA on appliance and not open source operating system and MTA.		
		The solution should be able to Identify graymail using the integrated graymail engine and apply appropriate policy controls		
		It should provide a secure and easy mechanism for end users to unsubscribe from unwanted graymail using cloud-based Unsubscribe Service		
		The file system should be purpose built and optimized for Messaging Queuing.		
		The solution should support both inbound and outbound email traffic control on single system		
		The MTA should support been built by stack less programming language that helps to improve the overall performance of the MTA by opening more threads resulting in more number of concurrent SMTP connections.		
		The MTA should maintain separate queues for each destination domain to avoid single queue issues.		
		The MTA should support the ability to set the retry schedule on a per domain basis.		
		The MTA should be able to send multiple messages per connection and be able to open multiple connections per host.		
		The MTA should support RFC 2821 compliant Simple Mail Transfer Protocol (SMTP) to accept and deliver messages.		

		The solution should support ability to perform SMTP session control and traffic rate limiting according to sender's IP address/range, domain or email reputation. The solution should be able to assign maximum SMTP sessions per IP address on appliance		
		The solution should be able to communicate with OpenLDAP, Active Directory or other LDAP servers to identify invalid recipients		
		The solution should perform SMTP conversational bounce for invalid recipients (prevent Non-Delivery Report Attack)		
		The Directory harvest prevention should control the maximum number of bounces per hour due to invalid email recipients according to sender's IP address/range, domain and email reputation		
		The directory harvest attack prevention should allow administrator to define limit on number of invalid recipient requests that can be accepted.		
		The reputation based filtering should support one of the biggest web and email traffic monitoring network for sender reputation		
		The solution should allow administrator to apply policies such as blocking known bad senders, throttling suspicious senders and allowing trusted senders based on reputation score assigned from reputation database		
		The reputation based scoring architecture should function at TCP conversation level and not after acceptance of email, to increase the overall performance & availability of the messaging infrastructure		
		The solution should support creation of customized sender groups and apply customized mail flow policies to each sender group.		
		Blacklist (IP, Domain, Reputation)		
		Whitelist (IP, Domain, Reputation)		
		Sender and Recipient address whitelist and blacklist		
		The solution should be able to block, accept, throttle, reject and TCP refuse based on:-		
		- Sender IP, IP range		
		- Domain		
		- Email Reputation score from reputation filtering		
		- DNS List		
		- Connecting host PTR record		
		- Connecting host PTR record lookup fails due to temporary DNS failure		
		- Connecting host reverse DNS lookup (PTR) does not match the forward DNS lookup (A)		
		Rate limit control by IP address, domain and sender's reputation		
		- Maximum Recipients per period traffic control		
		- Ability to define traffic flow based on time period down to minutes (say 15 minutes)		
		Real-Time Mail Flow Monitoring		
		(provide details of traffic flow down to per domain and IP address)		

		Statistics on Invalid Recipients, Stopped by Reputation, Spam and Virus Detected, and Cleaned Messages (Per Domain and IP address)		
		Should be able to provide last hour, last day, last week and last month statistics on blocked messages by rejected connection, spam and virus messages detected		
		To combat misdirected bounce attacks, the solution should support bounce verification tag to replace envelope sender for all outgoing messages; if a bounce arrives that doesn't contain the tag then it is discarded. Legitimate bounces should be delivered.		
		The solution should support assigning different IP addresses on single appliance to allow different host identities and also own traffic flow policy and sender groups (each IP address represents one department or one faculty MX host)		
		Each IP address should be able to respond with different SMTP response and banner (e.g. 220 mx.abc.com for IP address A, 220 mx.xyz.net)		
		The solution should support customized SMTP banner, hostname and response code per IP address or sender group		
		The solution should support multiple domains per IP address or multiple domains using different IP address on single appliance		
		The solution should support Per User or User Group Policy (Based on sender/recipient address/domain or LDAP group, i.e. single email to multiple recipients can be processed with different policies)		
		Should support single view of all user policies for easier management		
		The policy at SMTP conversation level should be able to perform reverse DNS domain lookup and assign policy per sender basis.		
		Per Sender Policy settings on:-		
		o Maximum Messages per connection		
		o Maximum Recipients per message		
		o Maximum message size		
		o Maximum Concurrent sessions per IP address		
		o TLS enforcement and preferred option		
		o SMTP Authentication enforcement and preferred option		
		Attachment Filtering (File attachment detection by): -		
		o true file type,		
		o file size,		
		o file name,		
		o file extension		
		o MIME type		
		Should be capable of the actions of :		
		o Ability to quarantine		
		o duplicate and quarantine		
		o strip attachment		
		o BCC		

		o redirection of email to another host or another recipient replacing the whole message		
		o just attachment with predefined message notification template		
		The solution should provide capability of the appliance to perform recipient validation by querying an external SMTP server prior to accepting incoming mail for the recipient		
		Sender Verification based on connecting IP address DNS PTR record and also envelope sender address		
		Should support:		
		o LDAP routing,		
		o masquerading,		
		o recipient address verification		
		o SMTPAUTH using LDAP		
		LDAP should be query based and not synchronization based for better performance.		
		The solution should support chained LDAP queries that will run in succession.		
		The solution should support LDAP referrals i.e. When using LDAP referral's, the original query gets referred to another LDAP server.		
		The solution should support LDAP caching on the appliance.		
		Per quarantine area access control and ability to control user name and password of quarantine areas so that some quarantine areas can only access by authorized personnel (e.g. "Confidential" Quarantine Area for Security Administrator, HR, etc.)		
		The solution should provide separate Quarantine areas for different functionalities such as:		
		Dedicated Spam Quarantine to quarantine spam/suspect-spam		
		Virus Quarantine – to quarantine virus files		
		Outbreak Quarantine – Dynamically quarantine zero day threats		
		Policy Quarantine – to quarantine based on policy such as "quarantine outbound Resume's"		
		Flexibility to create additional Policy quarantines		
		The appliance platform OS should support both command line and GUI content filters to allow complex policy control requirements.		
		The solution should support:		
		Keyword checking		
		Weighted content dictionaries		
		Keywords embedded into documents		
		Keywords embedded into zip archives		
		Inbuilt identifiers such as SSN, Credit Cards, JCB card number, etc		
		File Types		
		MIME types		

		The solution should support trusted relay so that original senders' IP address can be identified from "Received" headers or other email headers (when appliance is not first layer mail gateway)		
		Multi-layer Anti-spam filter:		
		TCP connection level Reputation Filtering (Sender IP/domain)		
		On Box Anti-spam Filtering		
		Allow integrated use of different vendor anti-spam engine		
		The spam rules should be automatically updated every 5 minutes		
		Solution should be able to distinguish between spam and marketing mail from a legitimate source		
		Real-Time Mail Policy Change on Possible Spammers and Hackers (by Per Domain and IP address) so as to change the policy to block/throttle those bad senders		
		Quarantine:		
		On-box quarantine for administrator		
		Individual User/Password Access Control for spam Quarantine Area		
		End User Quarantine Support with LDAP/AD/IMAP/POP authentication support		
		Outlook Plug-in support for reporting missing spam, false positives, phishing and virus emails		
		The solution should support for dual virus scanning available within the appliance		
		The solution should provide protection against zero-day and targeted attacks. It should be able to dynamically analyze message attachments for malware without sending files to cloud		
		The proposed solution should include Anti-APT / Next Generation detection ability to quarantine emails suspected to been infected with malware		
		The proposed solution shall support the ability to hold the email until sandbox analysis is complete and the threshold shall be configurable		
		The proposed Email Security Appliance MUST NOT support webmail module since it will allow remote attackers to perform directory traversal vulnerability attack		
		The proposed solution should be able to aid in incident response mechanism within the environment including (and not limited to the following):		
		1. Infected users with offending email		
		2. Scope of the malware threats including reports on number of users involved, email sender and recipients, first detections and detailed email messaging history		
		3. Reverse DNS hostname with IP information		
		Proposed email advance malware solution should allow user to manually download the sample for further analysis and forensic purposes.		
		The solution should provide virus outbreak prevention		
		The solution should provide the URL defense service to:		

		o Re-write the original suspicious URL in the mail body to another URL		
		o On clicking the re-written URL, the browser session should pass through a cloud based Web security scanning infrastructure of the same OEM		
		Automatic quarantine and release of quarantined messages not falling into new virus/worm characteristics upon outbreak rule update and before virus signature update		
		Configurable update period down to every 5min		
		Solution should support attachment and Compressed File scanning		
		Support both Internet Root DNS servers or local DNS servers		
		Support multiple DNS servers according to destination domain(s), i.e. DNS A server for Domain A, and DNS B server for Domain B		
		The solution should support following for system monitoring: -		
		SNMP v2/v3, MIB-II, XML, Syslog support		
		The solution should support following for alerts: -		
		Email-based, SNMP Trap		
		Solution should support control from which ip addresses users can access to manage the appliance		
		The solution should support following updates:		
		System updates (able to upgrade and restore email service within 5 minutes), Automatic Spam definition updates, Automatic Virus definition updates		
		The solution should support outbound SMTP over TLS based on destination domains or system wide		
		The solution should support outbound SMTP authentication		
		The solution should support policies to sign outgoing emails based on domain key and allow to sign by different domain keys based on sender domain		
		The administrator should be able to define different bounce profiles for destination domains (retry frequency, maximum retry period, etc.) to minimize bandwidth for non-important emails		
		The solution should support for end user to create block and safe lists. Safe lists allow a user to ensure that certain users or domains are never scanned with anti-spam scanning engines, while block lists ensure that certain users or domains are rejected or quarantined.		
		The solution should support provision to authenticate users using RADIUS or LDAP for logging into appliance for management purpose		
		If SMTP authentication is used to send messages, the solution should support facility to check messages with spoofed headers.		
		The appliance should support the use of IPv6 for:		
		o Appliance interfaces		
		o Gateways (default routes)		
		o Static routes		
		o SMTP Routes		

		o Querying external SMTP server with IPv6 address (for Recipient validation)		
		o IPv6 Sending hosts		
		o Content Filters		
		o Sending to IPv6 destinations		
		o Report searches		
	Design and Implementation Scope	The OEM will prepare the entire design of the BCC Security LAB keeping in mind the compliance requirements and operational requirements.		
		The OEM Validated Design should take into consideration - scalability, modularity, and resiliency aspects of the Security Lab as well as optimization from space, power and cooling perspective.		
		Respective OEM to also ensure that the final deployment is done basis the OEM specified and validated design standards and best practices.		
	Manufacturer's part number	Bidder should submit BOQ of proposed device/solution including the details part numbers and Manufacturer's Warranty part number.		
		Bidder must submit the required performance document and feature compliance reference document for the proposed device/solution.		
	Warranty	Manufacturer's warranty part number should be mentioned, minimum 3 (Three) years warranty should be provided for this unit from the date of commissioning		

Item-19: Web Security System				
SL. #	**Product Names/Items**	**Technical Specifications**	**UOM**	**QTY**
19	**Quality**	ISO 9001/9002 for manufacturer, FCC Class A/B for quality assurance	Lot	1
	Brand	To be mentioned by the bidder		
	Model	To be mentioned by the bidder		
	Part No	Bidder should submit BOQ of proposed device including the details part numbers. Bidder should submit the required feature & performance compliance document for the proposed solution.		
	Solution Requirement and Functionality	The solution should have 100 users license for web security control with web reputation, web filtering, anti-phishing, web malware protection from day 1.		
		The solution should include Web Proxy, Caching, Web based Reputation filtering, URL filtering, Antivirus and Anti-malware based solution.		
		Bidder must propose the required hardware & software with related resource for Mail Security System.		
	Operating System & Security	The Solution should be provided with hardened Operating System and secure from vulnerabilities functionality.		
	Support multiple deployment options	The solution should allow deploying the solution explicit proxy as well as transparent mode together.		

	Proxy Chaining	The solution should support proxy configuration in a Chain. The Lower end proxies at spoke locations should be able to forward the request to an Higher end proxies at Hub Location forming a Chain of Proxies		
	DNS Splitting	The solution should support configuration to use Split DNS. It should be able to refer to different DNS for Different Domains e.g. root DNS for all external domains and internal DNS for organization		
	IP Spoofing support in transparent mode deployments	The solution should have facility to do IP spoofing. When enabled, requests originating from a client should retain the client's source address and appear to originate from the client instead of the appliance. This is useful in scenarios where policies are based on original IP and logging/reporting is required to track activity of individual IP basis.		
	High Availability	Should support active/standby High Availability mode		
	Proxy support	The proposed solution should be a Fast Web Proxy and should support HTTP, FTP and HTTPS proxy.		
	HTTPS Decryption	The solution should support HTTPS decryption		
	HTTPS decrypted traffic scanning	The solution should support scanning of the https decrypted traffic by the on-board anti-malware and/or anti-virus engines.		
	HTTPS decryption controls	The solution should provide the flexibility of deciding whether to decrypt https traffic or not to the solution administrator. The solution should offer three aspects to decide. These are:		
		1) URL category based decryption		
		2) Web Reputation based decryption		
		3) Default action for the specific policy		
	HTTPS decryption policy	HTTPS decryption should provide flexibility to have multiple decryption policies and should not be just a Global action		
	Protocol Tunneling	Should support the functionality to block applications that attempts to tunnel non-HTTP traffic on ports typically used for HTTP traffic.		
		Should support the functionality for blocking non-SSL traffic on SSL ports & should also support the functionality to tunnel the transaction.		
	Native FTP protection	The solution should act as an FTP proxy and enable organizations to exercise		
		granular control, including: allow/block FTP connections,		
		restrict users/groups, control uploads/downloads, and		
		Restrict sent/received files to certain types or sizes.		
	File download and size restrictions	The solution should be capable of blocking specific files downloads and based on size and per user group basis. It should also provide option to block object using MIME File types.		
	IP based Access Control	The solution should allow administrator to define access to internet based on IP addresses, range of IP addresses, subnet and CIDR basis. It should also support to be forced for Authentication from Specific IP addresses, Subnet or CIDR's		

	Multiple Authentication Server Support	The solution should support Multiple Auth Servers / Auth Failover using Multi Scheme Auth (NTLM and LDAP). It should also support authentication exemption.		
	Application and Protocol Control	The solution should support granular application control over web e.g. Facebook controls like block file upload, block posting text, enforcing bandwidth limits on application types.		
	Layer 4 Traffic Monitoring	Should support detection of Phone Home attempts occurring from the entire Network. It should also detect the PC's that are already infected with Malware in the Network across all network ports that attempts to bypass port 80.		
	Bandwidth restrictions	The solution should support providing bandwidth limit/cap for streaming media application traffic. This should be possible at the Global level as well as at a per policy level.		
	Anti-Malware / Malware Protection	The solution should have support for at least 1 industry known Anti Malware/Anti-Virus engine that can scan HTTP, HTTPS and FTP traffic for web based threats, that can range from adware, browser hijackers, phishing attacks to more malicious threats such as Rootkits, Trojans, worms, system monitors and Key loggers and as defined by the organizations policy. Bidder need to mention the antimalware engine.		
		With dual AV/Anti-Malware engine scanning when a URL causes different verdicts from the scanning engine the solution should perform the most restrictive action.		
		The AV/Malware engines should protect at least against the follow types of malware/threats: Adware, Browser Helper Object, Commercial system monitor software, Dialer, Generic spyware, Hijacker, Phishing URL, potentially unwanted applications, Trojan downloader, virus, worm etc.		
	Web Reputation	The solution should provide Web Reputation Filters that examine every request made by the browser (from the initial HTML request to all subsequent data requests) – including live data, which may be fed from different domains to assign a web based score to determine the likelihood that it contains URL based malware.		
	Web Reputation parameters	The Web Reputation Filters should have capability to analyze more than 100 different web traffic and network-related parameters to accurately evaluate the trustworthiness of a URL or IP address.		
		Solution should also support in participating by providing information to the cloud based servers to increase the efficacy & reputation based scoring.		
	Customizable Web Reputation	The solution should have customizable setting in the Web Based Reputation Services, like Allow, Scan and Block based on the scoring settings by the Administrator.		
	Incoming/ Outgoing Traffic scanning	The solution should scan for Incoming and outgoing traffic.		
	Outbound connection control on all ports and protocols	The solution shall provide option to scan all ports at wire speed, detecting and blocking spyware activity trying to connect to the outside Internet. By tracking all 65,535 network ports and all protocols, the solution shall effectively mitigate malware that attempts to bypass Port 80		
	URL filtering	The solution should have an inbuilt URL filtering functionality with multiple pre-defined categories.		

	Custom URL filtering	The solution should support creation of custom URL categories for allowing/blocking specific destinations as required by the Organization.		
	URL Filtering Options	The web Proxy should support following actions like allow, monitor, block, time-based access. Should also support displaying a warning page but allows the user to continue clicking a hypertext link in the warning page.		
	Dynamic Categorization	Provision should be available to enable Real Time Dynamic categorization that shall classify in real time in case the URL the user is visiting is not already under the pre-defined or custom categories database.		
	Reporting Miss-categorization	The solution should have facility for End User to report Miss-categorization in URL Category.		
	URL check & submission	Support portal should give facility to end user to check URL category and submit new URL for categorization		
	Filtering Content	Solution should support filtering adult content from web searches & websites on search engines like Google.		
	Signature based application control	The solution should support signature based application control. For instance, it should allow Facebook but should support blocking of only chat or file transfer or playing games within Facebook. This blocking should be based on signature and not URL. The application signature database should be updated periodically by the vendor. Mention the number of signatures available in the current release or mention the number of web based applications that can be blocked by the current signature set.		
	End User Notification	Solution should support following end user notification functionalities.		
		The proxy should support the functionality to display a custom message to the end user to specify the reason the web request is blocked.		
		When the website is blocked due to suspected malware or URL-Filters it should allow the end user to report that the webpage has been wrongly misclassified.		
		The solution should support the functionality of redirecting all notification pages to a custom URL to display a different block page for different reasons.		
		Should support the functionality to force users to explicitly agree to the terms and conditions for browsing the World Wide Web from the organization's network to let the user know that the Organization is monitoring their web activity.		
	Remote support	The remote support from principal company should be available via India Toll Free and Email. The Support Portal access should be provided for Case management, knowledgebase, new version information, tools etc.		
	Secure Remote Access	The Support Engineers should be able to login to solution using secure tunneling methods such as SSH for troubleshooting purposes		
	Diagnostic Tools	The solution should have diagnostic network utilities like telnet, traceroute, nslookup and tcpdump/packet capture.		
	Updates and	The solution should provide seamless version upgrades and updates.		

	Upgrades	Solution should support a web interface that includes a tool that traces & can simulate client requests as if they were made by the end users and describes Web Proxy processes the request for troubleshooting purpose. It should support simulating HTTP GET & POST requests.		
	Secure Web Based management	The solution should be manageable via HTTP or HTTPS		
	CLI based management	The solution should be manageable via command line using SSH		
	Web Logs	The Proxy Log should be scalable. The log formats shall include Apache, Squid and W3C.		
	Log retention & rollover	Solution should support automatic "rollover" & archive the log file when it reaches admin defined maximum file-size or time interval like daily/weekly rollover of logs.		
		Should support compressing rolled over log files before storing them on disk to reduce disk space consumption.		
	Log transfer	The solution should support following mechanism to transfer log files:		
		Should support remote FTP client to access the solution to retrieve log files using an admin or operator user's username and password.		
		Periodically pushing log files to an FTP server		
		Periodically pushes log files using the secure copy protocol to an SCP server on a remote computer		
		Sending logs to a remote Syslog server confirming to RFC 3164.		
	Retention Period	The retention period should be customizable. Options should be provided to transfer the logs to an FTP server using FTP or SCP.		
	User Reports	Informative and exhaustive set of reports on User Activity and URL filtering activities (GUI to report past activity, top usage users and top malware threat)		
	Bandwidth Reports	Reports on Bandwidth Consumed / Bandwidth Saved		
	Detailed logging	Product to maintain detailed proxy access logs that can be searched via filters, for easy location of any desired access of the user and to see how the product dealt with it		
	Off Box Reporting	Solution should also support centralized reporting.		
	L4 traffic reports	Detailed report on an IP basis should be provided on the L4 traffic monitoring / Network Layer Malware Detection.		
	Blocked by reputation & malware reports	It should support reporting web requests blocked due to web reputation & blocked by malware		
	Report Formats	Solution should support generating a printer-friendly formatted pdf version of any of the report pages. Should also support exporting reports as CSV files.		
	Scheduling of Reports	Solution should support to schedule reports to run on a daily, weekly, or monthly basis.		
	System Reports	Should support system reports to show CPU usage, RAM usage, percentage of disk space used for reporting & logging.		

	Updates and Upgrades	Support should cover all upgrades for the time period the licenses and support purchased from principal vendor		
	IP V6 Support	Should have the ability to proxy, monitor, and manage IPv6 traffic.		
	Design and Implementation Scope	The OEM will prepare the entire design of the BCC Security LAB keeping in mind the compliance requirements and operational requirements.		
		The OEM Validated Design should take into consideration - scalability, modularity, and resiliency aspects of the Security Lab as well as optimization from space, power and cooling perspective.		
		Respective OEM to also ensure that the final deployment is done basis the OEM specified and validated design standards and best practices.		
	Manufacturer's part number	Bidder should submit BOQ of proposed device/solution including the details part numbers and Manufacturer's Warranty part number.		
		Bidder must submit the required performance document and feature compliance reference document for the proposed device/solution.		
	Warranty	Manufacturer's warranty part number should be mentioned, minimum 3 (Three) years warranty should be provided for this unit from the date of commissioning		

Item-20: Virtual Firewall				
SL. #	**Product Names/Items**	**Technical Specifications**	**UOM**	**QTY**
20	**Quality**	ISO 9001/9002 for manufacturer, FCC Class A/B for quality assurance	Set	1
	Brand	To be mentioned by the bidder		
	Model	To be mentioned by the bidder		
	Part No	Bidder should submit BOQ of proposed device including the details part numbers. Bidder should submit the required feature & performance compliance document for the proposed solution.		
	Virtual Firewall Requirement	The virtual appliance should be capable of providing Firewall and VPN Services		
		Firewall performance (Large packets) 1 Gbps with multiprotocol performance of 500 Mbps		
		Firewall should be capable configuring Policies using Command Line (CLI) as a last resort in case of Emergency.		
		Firewall should support maximum 98,000 concurrent connections or more		
		Firewall should support maximum 19000 new connections per second (cps) or more		
		Should deliver VPN throughput of 120 mbps or more		
		Firewall should support memory up to 2 GB for better and faster processing.		
		Bidder must propose the required hardware & software with related resource for Firewall Security System.		

		1. The firewall shall be deployed in high availability mode (hot stand-by redundancy), have fault tolerance and shall provide Stateful failover		
		2. The firewall shall have a powerful OS that is hardened and is based upon minimal feature sets.		
		3. There shall be support for traffic-based and for user based access control.		
		4. The firewall shall allow configuration of policy that governs the rules according to which the firewall handles the traffic.		
		5. The broad default policy for the firewall for handling inbound traffic shall be to block all packets and connections unless the traffic type and connections have been specifically permitted		
		6. It shall support SNMP (Simple Network Management Protocol) v 2.0 and v 3.0.		
		Should support translating between IPv4 and IPv6 for the following inspections:		
		•DNS		
		•FTP		
	Firewall General Features	•HTTP		
		•ICMP		
		Network address translation (NAT) shall be supported so that the private IP addresses of hosts and the structure of an internal network can be concealed by the firewall.		
		1. Network Address Translation (NAT) shall be configurable as 1:1, 1: many, many: 1, many: many, flexible NAT (overlapping IPs). Reverse NAT shall be supported.		
		2. Port address translation/Masquerading shall be provided for.		
		3. Dynamic Host Configuration Protocol (DHCP) over Virtual Private Network (VPN) shall be supported for dynamic allocation of IP addresses.		
		4. Virtual LAN (VLAN) support with minimum 150 virtual interface, WAN support, LAN/DMZ support		
		5. The firewall IP stack shall be IPv6 ready.		
		6. Policy consistency across the DC for VM mobility		
		7. LACP with vPC support		
		8. VxLAN support		
		1) The firewall shall mask the internal network from the external world.		
	Attack Protection	2) The firewall shall provide robust access control capability and be fast in making access control decisions. Access Control shall be done based on criteria such as source, destination IPs, port number, protocol, traffic type, application, date information (day of week, time of day), etc.		
		3) Multi-layer, Stateful, application-based filtering shall be done		

		4) It shall provide network segmentation features with powerful capabilities that facilitate deploying security for various internal, external and DMZ (Demilitarized Zone) sub-groups on the network, to prevent unauthorized access.		
		5) Ingress/egress filtering capability shall be provided.		
		6) There shall be support for detection of reconnaissance attempts such as IP address sweep, port scanning etc.		
		7) Firewall itself shall be resistant to attack and shall have protection against firewall evasion techniques.		
		8) Some basic attack protection features listed below but not limited to :		
		a. Maximum no of protections against attacks that exploit weaknesses in the TCP/IP protocol suite		
		b. It shall enable rapid detection of network attacks		
		c. TCP reassembly for fragmented packet protection		
		d. Brute force attack mitigation		
		e. SYN cookie protection, SYN Flood, Half Open Connections and NUL Packets		
		f. Protection against IP spoofing		
		g. Malformed packet protection		
		h. Java blocking, and real-time alerts		
		i. securely segregate individual guest VMs		
		j. enable monitoring of the traffic between VMs on the same physical host		
		k. protects against VM attacks initiated by VMs to other VMs on the same physical host		
		l. inspects traffic between VMs		
		1. The firewall shall support Internet Protocol Security (IPSec) & SSL		
		2. Key exchange with latest Internet Key Exchange (IKE), IKEv2, Public Key Infrastructure PKI (X.509) shall be catered to.		
		3. Site-to-site VPN tunnels: full-mesh / star topology shall be supported.		
	VPN Features	4. Support Latest Encryption algorithms including AES 128/192/256(Advanced Encryption Standards), 3DES(Data Encryption Standard) etc.,		
		5. Support Latest Authentication algorithms including SHA-1(Secure Hash Algorithm-1), SHA-2(Secure Hash Algorithm-2) etc.,		
		6. IPSec NAT traversal shall be supported.		
		7. Configuration of VPN shall be intuitive and user friendly.		
		8. VPN throughput should be at least 120 Mbps supporting 240 IPSec / SSL VPN peers		
	Management Capabilities	Firewall should support management of firewall policies via CLI, Telnet, SSH & inbuilt GUI management interface.		

		Firewall should support Syslog with the functionality of sending Syslog messages via email to different teams based on Syslog severity		
		Firewall should support SNMP logging & specify which messages are to be sent to SNMP servers		
		Firewall should support rate-limiting of Syslog messages to avoid Dos attacks on the firewall		
		Firewall should support the functionality of identifying issues quickly with continuous monitoring & providing notifications of potential problems in which a service request has been raised with all diagnostic data attached.		
		Firewall Graphical/Web management interface should support backing up & restoring configurations		
		Firewall GUI/Web Management should support inbuilt function to simulate network traffic to check firewall rules & for troubleshooting network access issues		
		Firewall should support packet capturing functionality to send the packet capture to ethereal/wire shark for detailed packet analysis		
	Design and Implementation Scope	The OEM will prepare the entire design of the BCC Security LAB keeping in mind the compliance requirements and operational requirements.		
		The OEM Validated Design should take into consideration - scalability, modularity, and resiliency aspects of the Security Lab as well as optimization from space, power and cooling perspective.		
		Respective OEM to also ensure that the final deployment is done basis the OEM specified and validated design standards and best practices.		
	Manufacturer's part number	Bidder should submit BOQ of proposed device/solution including the details part numbers and Manufacturer's Warranty part number.		
		Bidder must submit the required performance document and feature compliance reference document for the proposed device/solution.		
	Warranty	Manufacturer's warranty part number should be mentioned, minimum 3 (Three) years warranty should be provided for this unit from the date of commissioning		

Item-21: Virtual Intrusion Prevention System				
SL. #	**Product Names/Items**	**Technical Specifications**	**UOM**	**QTY**
21	**Quality**	ISO 9001/9002 for manufacturer, FCC Class A/B for quality assurance	Set	1
	Brand	To be mentioned by the bidder		
	Model	To be mentioned by the bidder		
	Part No	Bidder should submit BOQ of proposed device including the details part numbers. Bidder should submit the required feature & performance compliance document for the proposed solution.		
	Platform Requirement	The solution should be proposed with next-generation intrusion prevention, application identification/tracking/visibility with malware protection feature from day 1.		

		The detection engine must be capable of operating in both passive (i.e., monitoring) and inline (i.e., blocking) modes.		
		Should have minimum Inspected throughput of 500Mbps for all kinds of real word traffic.		
		Virtual appliance should support at least 6 Data virtual NICs		
		Should have separate dedicated interface for management		
		Proposed NGIPS should support Hypervisor or similar architecture.		
		The proposed vendor must have a track record of continuous improvement in threat detection and must have successfully completed NSS Labs' IPS Methodology testing with a minimum exploit blocking rate of 95%		
		Bidder must propose the required hardware & software with related resource for Virtual Intrusion Prevision Security.		
	Next-Generation IPS Feature Requirement	Should have the capability of passively gathering information about virtual machine traffic, network hosts and their activities, such as operating system, services, open ports, client applications, and vulnerabilities, to assist with multiple activities, such as intrusion event data correlation, elimination of false positives, and policy compliance.		
		Should be capable of dynamically tuning IDS/IPS sensors (e.g., selecting rules, configuring policies, updating policies, etc.) with minimal human intervention.		
		Should be capable of automatically providing the appropriate inspections and protections for traffic sent over non-standard communications ports.		
		Should be able to link Active Directory and/or LDAP usernames to IP addresses related to suspected security events.		
		Should be capable of detecting and blocking IPv6 attacks.		
		The Solution must have the capability to quarantine end point		
		Solution should support full-featured NBA capability to detect threats emerging from inside the network. This includes the ability to establish "normal" traffic baselines through flow analysis techniques (e.g., NetFlow/Sflow) and the ability to detect deviations from normal baselines.		
		The solution must provide IP reputation feed that comprised of several regularly updated collections of poor reputation of IP addresses determined by the proposed security vendor		
		The solution should be able to identify, decrypt and evaluate SSL traffic		
		Solution must support IP reputation intelligence feeds from third party and custom lists of IP addresses including a global blacklist.		
		Should support URL and DNS threat intelligence feeds to protect against threats		
		Should support Reputation- and category-based URL filtering offering comprehensive alerting and control over suspect web traffic and enforces policies on more than 270 million of URLs in more than 75 categories.		
		Solution must be capable of defending against IPS-evasion attacks by automatically using the most appropriate defragmentation and stream reassembly routines for all traffic based on the characteristics of each destination host.		

		Solution must be capable of employing an extensive set of contextual information (e.g., pertaining to the composition, configuration, and behavior of the network and its hosts) to improve the efficiency and accuracy of both manual and automatic analysis of detected events.		
		Should support safe search for YouTube EDU enforcement		
		Solution must be capable of passively gathering details unique to mobile devices traffic to identify a wide variety of mobile operating systems, mobile applications and associated mobile device hardware.		
		Should support more than 4000 application layer and risk-based controls that can invoke tailored intrusion prevention system (IPS) threat detection policies to optimize security effectiveness.		
		Solution should support capability of providing network-based detection of malware by checking the disposition of known files in the cloud using the SHA-256 file-hash as they transit the network from day 1 and in future the solution should support the capability to do dynamic analysis on premise on purpose built-appliance if required.		
		Solution OEM must have its own threat intelligence analysis center and should use the global footprint of security deployments for more comprehensive network protection.		
		The detection engine should support capability of detecting and preventing a wide variety of threats (e.g., malware, network probes/reconnaissance, VoIP attacks, buffer overflows, P2P attacks, etc.).		
		Should be able to identify attacks based on Geo-location and define policy to block on the basis of Geo-location		
		The detection engine should support the capability of detecting variants of known threats, as well as new threats		
		The detection engine must incorporate multiple approaches for detecting threats, including at a minimum exploit-based signatures, vulnerability-based rules, protocol anomaly detection, and behavioral anomaly detection techniques. Identify and explain each type of detection mechanism supported.		
		Should support Open based Application ID for access to community resources and ability to easily customize security to address new and specific threats and applications quickly		
	Management	The management platform must be accessible via a web-based interface and ideally with no need for additional client software		
		The management platform must provide a highly customizable dashboard.		
		The management platform must be capable of integrating third party vulnerability information into threat policy adjustment routines and automated tuning workflows		
		The solution must be capable of passively gathering user identity information, mapping IP addresses to username, and making this information available for event management purposes.		
		The solution must be capable of significantly reducing operator effort and accelerating response to threats by automatically prioritizing alerts, ideally based on the potential for correlated threats to successfully impact the specific hosts they are directed toward		

		The management platform must be capable of role-based administration, enabling different sets of views and configuration capabilities for different administrators subsequent to their authentication.		
		Should support REST API for monitoring and configuration programmability		
		The management platform must provide multiple report output types or formats, such as PDF, HTML, and CSV.		
		The management platform must support multiple mechanisms for issuing alerts (e.g., SNMP, e-mail, SYSLOG).		
		The management platform must provide robust reporting capabilities, including a selection of pre-defined reports and the ability for complete customization and generation of new reports.		
		The management platform must risk reports like advanced malware, attacks and network		
		The management platform must include an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to enable events and log data to be shared with external network and security management applications, such as Security Information and Event Managers (SIEMs), and log management tools.		
	Design and Implementation Scope	The OEM will prepare the entire design of the BCC Security LAB keeping in mind the compliance requirements and operational requirements.		
		The OEM Validated Design should take into consideration - scalability, modularity, and resiliency aspects of the Security Lab as well as optimization from space, power and cooling perspective.		
		Respective OEM to also ensure that the final deployment is done basis the OEM specified and validated design standards and best practices.		
	Manufacturer's part number	Bidder should submit BOQ of proposed device/solution including the details part numbers and Manufacturer's Warranty part number.		
		Bidder must submit the required performance document and feature compliance reference document for the proposed device/solution.		
	Warranty	Manufacturer's warranty part number should be mentioned, minimum 3 (Three) years warranty should be provided for this unit from the date of commissioning		

Item-22: End-Point Malware Protection Software				
SL. #	**Product Names/Items**	**Technical Specifications**	**UOM**	**QTY**
22	**Quality**	ISO 9001/9002 for manufacturer, FCC Class A/B for quality assurance	Lot	1
	Brand	To be mentioned by the bidder		
	Model	To be mentioned by the bidder		
	Part No	Bidder should submit BOQ of proposed device including the details part numbers. Bidder should submit the required feature & performance compliance document for the proposed solution.		
	End Point Protection Solution	The bidder shall propose an endpoint based solution to protect at least 50 endpoints/devices from Advanced Targeted Attacks and Advanced Persistent Threats.		

	Feature	The proposed solution shall work on a signature-less mechanism to stop threats without relying on a database to be present at the endpoint		
		The proposed solution shall work as an independent module without relying on other endpoint and network systems for its functionality		
		The proposed solution shall be capable of working along with all leading endpoint anti-virus vendors without needing to replace them		
		The proposed solution shall utilize layered and defense in depth approach, wherein the solution cannot be of the same make as existing endpoint AV		
		The proposed endpoint solution should support detecting of all malware types, both known and unknown. The movement of all known and unknown malware should be tracked and reported across the endpoints.		
		The proposed endpoint solution should be able to support continuous and root cause analysis to help in triaging of security incidents.		
		Security vendor must have a dedicated research organization that is focus on vulnerability research and should actively contribute to discoveries of new vulnerabilities exploited in the wild.		
		Software footprint should be small <100MB and must support interactive and/or silent install		
		Endpoint software must be easy to deploy and support (not limited to) deployment through 3rd party systems management tools		
		Root cause analysis on a suspected machines should include the following capability:		
		- Sequential and chronological trace of events with details including host, username, IP, client application involved		
		- Details should highlight which file/process/services that affected		
		Proposed endpoint software should support malware tracking and provide visualization at the network level: systems and affected users, patient zero, and method/point of entry.		
		Proposed system must support continuous and persistent monitoring of files to detect polymorphic and time bound malware whenever they start turning bad and shall not be only an on-demand scan mechanism		
		Proposed endpoint software must be capable to block CnC communications and dropper activity and contain the spread of malware		
		Remediation at endpoints for incident response should include (and not limited to):		
		- Track and capture files on suspected machine with option for lookups on suspected devices		
		- Block of files / process / services that are showing malicious behaviors		
		- Dropper detection and blocking of downloads via URL / sites		
		- Submit suspected malicious files for further analysis		
		The proposed solution shall have the capability to quarantine the malicious application/program/file automatically without quarantining the entire user machine from network which would affect business productivity of the user		
		The proposed solution shall have the capability to work with Indicators of Compromise (IOC's)		

		The proposed solution shall provide the capability to write/upload custom IOC's		
		The proposed solution shall provide details to enable forensic analysis of incidents		
		The solution shall be capable of working in Windows, Windows Server, Mac, Linux Redhat & CentOS operating systems		
		The endpoint solution shall be able to pinpoint vulnerable versions of popular applications installed in Endpoints		
		The proposed solution shall be able to identify the threat root cause of incidents, child processes of malwares and parent file disposition		
	Design and Implementation Scope	The OEM will prepare the entire design of the BCC Security LAB keeping in mind the compliance requirements and operational requirements.		
		The OEM Validated Design should take into consideration - scalability, modularity, and resiliency aspects of the Security Lab as well as optimization from space, power and cooling perspective.		
		Respective OEM to also ensure that the final deployment is done basis the OEM specified and validated design standards and best practices.		
	Manufacturer's part number	Bidder should submit BOQ of proposed device/solution including the details part numbers and Manufacturer's Warranty part number.		
		Bidder must submit the required performance document and feature compliance reference document for the proposed device/solution.		
	Warranty	Mentioning Manufacturer's warranty part number should be quoted, minimum 3 (Three) years warranty should be provided for this unit from the date of commissioning		

Item -23: Security Management System				
SL. #	**Product Names/Items**	**Technical Specifications**	**UOM**	**QTY**
23	**Brand**	To be mentioned by the bidder	Set	1
	Model	To be mentioned by the bidder		
	Part No	Bidder should submit BOQ of proposed device including the details part numbers. Bidder should submit the required feature & performance compliance document for the proposed solution.		
	Management and Usability	The management platform must be capable of centralized, life cycle management for all sensors		
		The management platform must be delivered in physical HW / virtual platform		
		Bidder must propose the required hardware & software with related resource for Security Management Console Software.		
		The management platform must be capable of aggregating IDS/IPS events and centralized, real-time monitoring and forensic analysis of detected events.		
		The management platform must be accessible via a web-based interface and ideally with no need for additional client software.		
		The management platform must provide a highly customizable dashboard.		

		The management platform must be capable of integrating third party vulnerability information into threat policy adjustment routines and automated tuning workflows.		
		The management platform must be capable of role-based administration, enabling different sets of views and configuration capabilities for different administrators subsequent to their authentication.		
		The management platform must include a scheduling subsystem to facilitate automation of routine tasks, such as backups, upgrades, report creation, and policy application.		
		The management platform must include one or more default (i.e., pre-defined) detection policy configurations to help simplify initial deployment.		
		The management platform must be capable of grouping both sensors and policies to help simplify configuration management.		
		The management platform must provide the capability to easily view, enable, disable, and modify individual rules, as well as groups or categories of rules.		
		The management platform must be capable of automatically receiving rule updates published by the vendor and automatically distributing and applying those rule updates to sensors.		
		The management platform must be capable of backup and rollback for sensor configurations and the management platform itself.		
		The management platform must include flexible workflow capabilities for managing the complete life cycle of an event, from initial notification through to any response and resolution activities that might be required.		
		The management platform must provide the ability to view the corresponding detection rule for each detected event, along with the specific packet(s) that caused it to be triggered.		
		The management platform must support both internal and external databases/systems for storage of event data, logs, and other system-generated information.		
		The management platform must be capable of synchronizing time between all components of the system via NTP.		
		The management platform must be capable of logging all administrator activities, both locally and to a remote log server.		
		The solution must support LDAP for single sign-on to sensors and the management console.		
	Reporting and Alerting	The management platform must provide robust reporting capabilities, including a selection of pre-defined reports and the ability for complete customization and generation of new reports.		
		The management platform must allow quick report customization by importing from dashboards, workflows and statistics summaries.		
		The management platform must provide multiple report output types or formats, such as PDF, HTML, and CSV.		
		The management platform must support multiple mechanisms for issuing alerts (e.g., SNMP, e-mail, SYSLOG).		
	Third-Party Integration	The management platform must include an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to enable automatic response to threats by external components and remediation applications, such as routers, firewalls, patch management systems, etc.		

		The management platform must include an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to enable events and log data to be shared with external network and security management applications, such as trouble-ticketing systems, Security Information and Event Managers (SIEMs), systems management platforms, and log management tools.		
		The management platform must include an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to receive information from external sources, such as configuration management databases, vulnerability management tools, and patch management systems, for threat correlation and IT policy compliance purposes.		
		The management platform must include an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to export SNMP information to network management systems.		
		The management platform must include an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to obtain network intelligence (i.e., NetFlow/SFlow) from routers and switches.		
	Solution Requirement	The solution can manage at least 20 security devices like next-generation firewall & IPS etc.		
		The solution can support minimum 40,000 network server / hosts / users.		
		The solution can support minimum 8 million security/intrusion record events		
		Bidder must propose the required hardware & software with related resource for Security Management Console.		
	Design and Implementation Scope	The OEM will prepare the entire design of the BCC Security LAB keeping in mind the compliance requirements and operational requirements.		
		The OEM Validated Design should take into consideration - scalability, modularity, and resiliency aspects of the Security Lab as well as optimization from space, power and cooling perspective.		
		Respective OEM to also ensure that the final deployment is done basis the OEM specified and validated design standards and best practices.		
	Manufacturer's part number	Bidder should submit BOQ of proposed device/solution including the details part numbers and Manufacturer's Warranty part number.		
		Bidder must submit the required performance document and feature compliance reference document for the proposed device/solution.		
	Warranty	Mentioning Manufacturer's warranty part number should be quoted, minimum 3 (Three) years warranty should be provided for this unit from the date of commissioning		

Item -24: Network Behavior Analysis System				
SL. #	**Product Names/Items**	**Technical Specifications**	**UOM**	**QTY**
24	**Quality**	ISO 9001/9002 for manufacturer, FCC Class A/B for quality assurance	Set	1
	Brand	To be mentioned by the bidder		
	Model	To be mentioned by the bidder		
	Part No	Bidder should submit BOQ of proposed device including the details part numbers. Bidder should submit the required feature &		

		performance compliance document for the proposed solution.		
	General Requirements	The solution should be a purpose-built solution for security monitoring, threat prevention, and packaged security analytics. Should not be a log management solution		
		The solution should collect flow data continuously to do security threat and behavior analysis.		
		The solution should have capabilities like user identity tracking, relational flow maps, NAT stitching, layer 7 anomaly detection, and advanced investigation / forensics capabilities from day 1.		
	Network performance	Solution should provide application bandwidth utilization graph for various applications which should include bandwidth consumption for top hosts and trends on network bandwidth utilization.		
		Solution should probe the network in a manner so that impact on network performance is minimal.		
		Should support both in line and offline modes.		
		The tool should have a system for interactive event identification and rule creation		
		Devices / applications those do not support flows, the solution should be capable to generate its own flows for monitoring.		
		Solution should have facility to assign risk and credibility rating to events.		
		Solution should support traffic rate up to 1 Gbps		
		The solution should have console/management platform which can handle at least 5 Netflow / Sflow collector / aggregator.		
		The Flow collectors should have the ability to collect 1,000 flows per second from day 1 and scalable to at least 28,000 per second in future if required.		
		The Flow sensor should have the ability to collect 1,000 flows per second from day 1 and scalable to at least 28,000 per second in future if required.		
		The entire deployment of NBA solution should have the ability to support multiple collectors and the central controller should have the capability to scale up to 28,000 flows per second for near future		
		Bidder must propose the required hardware & software with related resource for Network Behavior Analysis System.		
	Minimum Requirement Description	Should have an automated discovery function to identify network devices and capture information such as IP address, OS, services provided, other connected hosts.		
		Should capture signature / heuristics based alerts and block the same		
		Should Identify the source of an attack and should not block legitimate users		
		Should identify worms through techniques such as identifying the use of normally inactive ports or identification of network scanning activities		
		The solution should be capable of detecting denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks including floods of all types (ICMP, UDP, TCP SYN, TCP NULL, IP NULL etc.), identify the presence of botnets in the network, identify DNS spoofing attack		

		etc.		
		Should be capable of conducting protocol analysis to detect tunneled protocols, backdoors, the use of forbidden application protocols etc.		
		Should utilize Anomaly detection methods to identify attacks such as zero-day exploits, self-modifying malware, attacks in the ciphered traffic or resource misuse or mis-configuration.		
		The solution should Integrates with Microsoft Active Directory, RADIUS, and DHCP to provide user Identity information in addition to IP address information throughout the system & allow groups based on Identity or Active Directory workgroup & Provides full historical mapping of User Name to IP address logins in a searchable format		
		Should support the capability to instruct network security devices such as firewalls to block certain types of traffic or route it to quarantine VLANS		
		Should support the capability to alert the admin and provide mitigation action like quarantine or block the endpoint or custom scripts like ACL push or block the further spread of the malware/worm while allowing legitimate traffic to continue		
		The system should be able to monitor flow data between various VLANS		
		Should support the capability to identify network traffic from high risk applications such as file sharing, peer-to-peer, etc.		
		Should support the capability to link usernames to IP addresses for suspected security events.		
		Should support the capability to extract user defined fields (including source and destination IPs, source and destination MAC address, TCP/UDP ports or ICMP types and codes, no. of packets and no. of bytes transmitted in a session, timestamps for start and end of session etc.) from captured packet data and then utilize fields in correlation rules.		
		Should support the capability Application profiling in the system and should also support custom applications present or acquired by the bank/customer		
		Solution should be compatible with a virtual environment.		
		The solution should provide access to raw as well as processed logs		
		Dashboard should have the facility to be configured according to user profile		
		System should support event forwarding for SMTP, SYSLOG & SNMP for high risk issues		
		The solution must allow analysis by grouping of network segments such as User VLAN, Management VLAN, Server Farms etc.		
		Solution should be able to track user's activities locally and remote network sites and should be able to report usage behavior across the entire network.		
		Solution should support ubiquitous access to view all reporting functions using an internet browser.		
		The solution should support the identification of applications tunneling on other ports		

		Solution should be able to collect security and network information of servers and clients without the usage of agents		
		The solution should be able to conduct de-duplication of redundant flow identified in the network to improve performance		
		The solution should have the ability to Stateful reassemble uni-directional flows into bi-directional conversations; handling de-duplication of data and asymmetry		
		The solution should support all forms of flows including but not limited to NetFlow, jflow, sflow, ipfix for udp etc.		
		The solution should be able to combine/stitch the flow records coming from different network devices like routers/switches/firewall that are associated with a single conversation and present them as a single bi-directional flow record		
		The solution should be able to stitch flows into conversations even when the traffic is NAT-ted by the firewall; clearly showing the original and translated IP address		
		The solution should be able to leverage external threat feeds for information about known CnC connections, botnets, Tor exit nodes, etc		
	Design and Implementation Scope	The OEM will prepare the entire design of the BCC Security LAB keeping in mind the compliance requirements and operational requirements.		
		The OEM Validated Design should take into consideration - scalability, modularity, and resiliency aspects of the Security Lab as well as optimization from space, power and cooling perspective.		
		Respective OEM to also ensure that the final deployment is done basis the OEM specified and validated design standards and best practices.		
	Manufacturer's part number	Bidder should submit BOQ of proposed device/solution including the details part numbers and Manufacturer's Warranty part number.		
		Bidder must submit the required performance document and feature compliance reference document for the proposed device/solution.		
	Warranty	Mentioning Manufacturer's warranty part number should be quoted, minimum 3 (Three) years warranty should be provided for this unit from the date of commissioning		

Item-25: Network Access Control and Authentication System				
SL. #	**Product Names/Items**	**Technical Specifications**	**UOM**	**QTY**
25	**Quality**	ISO 9001/9002 for manufacturer, FCC Class A/B for quality assurance	Set	1
	Brand	To be mentioned by the bidder		
	Model	To be mentioned by the bidder		
	Part No	Bidder should submit BOQ of proposed device including the details part numbers. Bidder should submit the required feature & performance compliance document for the proposed solution.		
	Network Access Control & Authentication	The Solution should provide a highly powerful and flexible attribute-based access control solution that combines authentication, authorization, and accounting (AAA); posture; profiling; and guest management services on a single platform.		

	Specification:	It should allow enterprises to authenticate and authorize users and endpoints via wired, wireless, and VPN with consistent policy throughout the enterprise		
		Provides complete guest lifecycle management by empowering sponsors to on-board guests		
		The propose solution should have 3 units of Network Access Control & Authentication system with 300 basic end-point access control license and 100 advance end-point access control license.		
		Bidder must propose the required hardware & software with related resource for Network Access Control & Authentication System.		
		Delivers customizable self service portals as well as the ability to host custom web pages to ease device and guest on-boarding, automate endpoint secure access and service provisioning, and enhance the overall end-user experience inside business-defined workflows		
		Offers comprehensive visibility of the network by automatically discovering, classifying, and controlling endpoints connected to the network to enable the appropriate services per endpoint		
		Addresses vulnerabilities on user machines through periodic evaluation and remediation to help proactively mitigate network threats such as viruses, worms, and spyware		
		Enforces security policies by blocking, isolating, and repairing noncompliant machines in a quarantine area without requiring administrator attention		
		Offers a built-in monitoring, reporting, and troubleshooting console to assist helpdesk operators and administrators streamline operations		
		Allows you to get finer granularity while identifying devices on your network with Active Endpoint Scanning		
		Augments network-based profiling by targeting specific endpoints (based on policy) for specific attribute device scans, resulting in higher accuracy and comprehensive visibility of what is on your network		
		Manages endpoint access to the network with the Endpoint Protection Service, which enables administrators to specify an endpoint and select an action - for example, move to a new VLAN, return to the original VLAN, or isolate the endpoint from the network entirely - all in a simple interface		
		Utilizes standard RADIUS protocol for authentication, authorization, and accounting (AAA).		
		Supports a wide range of authentication protocols, including PAP, MS-CHAP, Extensible Authentication Protocol (EAP)-MD5, Protected EAP (PEAP), EAP-Flexible Authentication via Secure Tunneling (FAST), and EAP-Transport Layer Security (TLS).		
		Offers a rules-based, attribute-driven policy model for creating flexible and business-relevant access control policies. Provides the ability to create fine-grained policies by pulling attributes from predefined dictionaries that include information about user and endpoint identity, posture validation, authentication protocols, profiling identity, or other external attribute sources. Attributes can also be created dynamically and saved for later use		
		Provides a wide range of access control mechanisms, including downloadable access control lists (dACLs), VLAN assignments, URL redirect, and Security Group Access (SGA) tagging.		

		Should have predefined device templates for a wide range of endpoints, such as IP phones, printers, IP cameras, Smartphones, and tablets.		
		It should allow Administrators to create their own device templates. These templates can be used to automatically detect, classify, and associate administrative-defined identities when endpoints connect to the network. Administrators can also associate endpoint-specific authorization policies based on device type.		
		The Solution should have capability to collect endpoint attribute data via passive network telemetry, querying the actual endpoints, or alternatively from the infrastructure via device sensors on switches.		
		Solution should allow end users to interact with a self-service portal for device on-boarding, providing a registration vehicle for all types of devices as well as automatic supplicant provisioning and certificate enrollment for standard PC and mobile computing platforms.		
		Should support full guest lifecycle management, whereby guest users can access the network for a limited time, either through administrator sponsorship or by self-signing via a guest portal. Allows administrators to customize portals and policies based on specific needs of the enterprise.		
		Verifies endpoint posture assessment for PCs connecting to the network. Works via either a persistent client-based agent or a temporal web agent to validate that an endpoint is conforming to a company's posture policies. Provides the ability to create powerful policies that include but are not limited to checks for the latest OS patches, antivirus and antispyware software packages with current definition file variables (version, date, etc.), registries (key, value, etc), and applications. Solution should support auto-remediation of PC clients as well as periodic reassessment to make sure the endpoint is not in violation of company policies.		
		Allows administrators to quickly take corrective action (Quarantine, Un-Quarantine, or Shutdown) on risk-compromised endpoints within the network. This helps to reduce risk and increase security in the network.		
		Enables administrators to centrally configure and manage profiler, posture, guest, authentication, and authorization services in a single web-based GUI console, and greatly simplifying administration by providing consistency in managing all these services.		
		Includes a built-in web console for monitoring, reporting, and troubleshooting to assist help-desk and network operators in quickly identifying and resolving issues. Offers comprehensive historical and real-time reporting for all services, logging of all activities, and real-time dashboard metrics of all users and endpoints connecting to the network.		
		Should support consistent policy in centralized and distributed deployments that allows services to be delivered where they are needed		
		Solution should have capability to determine whether users are accessing the network on an authorized, policy-compliant device.		
		Solution should have capability to establish user identity, location, and access history, which can be used for compliance and reporting.		
		Solution should have capability to assign services based on the assigned user role, group, and associated policy (job role, location, device type, and so on).		

		Solution should have capability to grant authenticated users with access to specific segments of the network, or specific applications and services, or both, based on authentication results.		
		Solution should have capability which allows users to add a device on a portal, where the device goes through a registration process for network access. Should allow users to mark as lost any device that you have registered in the network, and blacklist the device on the network, which prevents others from unauthorized network access when using the blacklisted device. Should have capability to reinstate a blacklisted device to its previous status in Device Portal, and regain network access without having to register the device again in the Devices Portal. Should also support removing any device in the enterprise network temporarily, then register the device for network access again later.		
		The portal used for Device registration should be customizable, allowing to customize portal theme by changing text, banners, background color, and images		
		Should provide a Registered Endpoints Report, which provides information about a list of endpoints that are registered through the device registration portal by a specific user for a selected period of time. The report should provide the following details		
		•Logged in Date and Time		
		•Portal User (who registered the device)		
		•MAC Address		
		•Identity Group		
		•Endpoint Policy		
		•Static Assignment		
		•Static Group Assignment		
		•Endpoint Policy ID		
		•NMAP Subnet Scan ID		
		•Device Registration Status		
		Solution should classify a client machine, and should support client provisioning resource policies to ensure that the client machine is set up with an appropriate agent version, up-to-date compliance modules for antivirus and antispyware vendor support, and correct agent customization packages and profiles, if necessary		
		Solution should support automatic provisioning of NAC agents		
		Solution should support periodic reassessment for clients that are already successfully postured for compliance.		
		Solution should support the following endpoint checks for compliance for windows endpoints:		
		Check operating system/service packs/hot fixes		
		Check process, registry, file & application		
		check for Antivirus installation/Version/ Antivirus Definition Date		
		check for Antispyware installation/Version/ Antispyware Definition Date		
		Check for windows update running & configuration		

		Solution should support following remediation options for windows endpoints:		
		File remediation to allow clients download the required file version for compliance		
		link remediation to allow clients to click a URL to access a remediation page or resource		
		Antivirus remediation to update clients with up-to-date file definitions for compliance after remediation.		
		Antispyware remediation to update clients with up-to-date file definitions for compliance after remediation.		
		Launch program remediation for NAC Agent to remediate clients by launching one or more applications for compliance.		
		Windows update remediation to ensure Automatic Updates configuration is turned on Windows clients per security policy		
		Solution should integrate with the following MDM vendors like: Airwatch, Good, Mobileiron, Zenprise, etc,		
		Solution should support configuring MDM policy based on the attributes like: DeviceRegisterStatus, DeviceCompliantStatus, DiskEncryptionStatus, PinLockStatus, JailBrokenStatus, Serial Number, Manufacturer, IMEI, OS Version & phone number, etc.		
		Solution should support receiving updated endpoint profiling policies and the updated OUI database as a feed from the OEM database.		
		Should support native supplicant profiles to enable users to bring their own devices into network. When the user logs in, based on the profile that you associate with that user's authorization requirements, solution should provide the necessary supplicant provisioning wizard needed to set up the user's personal device to access the network. This should be supported over Microsoft windows, Apple Mac and iOS and Android devices.		
		When endpoints are discovered on the network, they can be profiled dynamically based on the configured endpoint profiling policies, and assigned to the matching endpoint identity groups depending on their profiles.		
		Should support using a simple filter that you can use to filter endpoints. The quick filter filters endpoints based on field descriptions, such as the endpoint profile, MAC address, and the static status that is assigned to endpoints when they are created in the Endpoints page.		
		Should support an advanced filter that you can preset for use later and retrieve, along with the filtering results. The advanced filter filters endpoints based on a specific value associated with the field description. You can add or remove filters, as well as combine a set of filters into a single advanced filter.		
		Should support importing endpoints from a comma-separated values (CSV) file in which the list of endpoints appears with the MAC address and the endpoint profiling policy details separated by a comma.		
		Support for importing endpoints from LDAP server. Should allow to import MAC addresses and the associated profiles of endpoints securely from an LDAP server. Should support an LDAP server to import endpoints and the associated profiles, by using either the default port 389, or securely over SSL, by using the default port 636.		

		Should support multiple Admin Group Roles and responsibilities like Help Desk Admin, Identity Admin, Monitoring Admin, Network Device Admin, Policy Admin, RBAC Admin, Super Admin and System Admin		
		Should support Role-based access policies which are access control policies which allow you to restrict the network access privileges for any user or group. Role-based access policies are defined when you configure specific access control policies and permissions. These admin access policies allow you to customize the amount and type of access on a per-user or per-group basis using specified role-based access permission settings that apply to a group or an individual user.		
		Should support Identity source sequences, which defines the order in which the solution will look for user credentials in the different databases. Solution should support the following databases:		
		•Internal Users		
		•Internal Endpoints		
		•Active Directory		
		•LDAP		
		•RSA		
		•RADIUS Token Servers		
		•Certificate Authentication Profiles		
		Must be able to differentiate policy based on device type + authentication		
		Should have Ability to authenticate at least one phone and multiple users on the same switch port without interrupting service		
		Solution should support MAB and can further utilize identity of the endpoint to apply the proper rules for access. MacAddressBypass is typically used for devices which do not support 802.1x		
		Solution must support Non 802.1x technology on assigned ports and 802.1x technology on open use ports		
		Solution should provide support policy enforcement through VPN gateways		
		Solution must allow users access to the network in a worst case scenario in case of AAA server outages or any other reasons like WAN failure.		
		Should support authenticating Machines and users connected to the same port on the switch in a single authentication flow		
		Should support authenticating IP phones and users connected behind IP phones on the same physical port.		
		Solution should have profiling capabilities integrated into the solution in order to detect headless host. The profiling features leverage the existing infrastructure for device discovery. Should support the use of attributes from the following sources or sensors:		
		* Profiling using MAC OUIs		
		* Profiling using DHCP information		
		* Profiling using RADIUS information		
		* Profiling using HTTP information		

		* Profiling using DNS information		
		* Profiling using NetFlow information		
		* Profiling using SPAN/Mirrored traffic		
		Solution should support troubleshooting authentication issues by triggering session re-authentication to follow up with an attempt to re-authenticate again.		
		Should support session termination with port shutdown option to block an infected host that sends a lot of traffic over the network.		
		Should support the functionality to force endpoint to reacquire IP address that does not support a supplicant or client to generate a DHCP request after a VLAN change.		
		Troubleshooting & Monitoring Tools		
		Should support tools to run SHOW command on the network device.		
		Should support evaluation of the configuration of the device with the standard configuration.		
		Should support TCP dump utility & also support saving a TCP dump file.		
		Solution should support schedule reports to run and re-run at specific time or time intervals & send and receive email notifications once the reports are generated.		
	Design and Implementation Scope	The OEM will prepare the entire design of the BCC Security LAB keeping in mind the compliance requirements and operational requirements.		
		The OEM Validated Design should take into consideration - scalability, modularity, and resiliency aspects of the Security Lab as well as optimization from space, power and cooling perspective.		
		Respective OEM to also ensure that the final deployment is done basis the OEM specified and validated design standards and best practices.		
	Manufacturer's part number	Bidder should submit BOQ of proposed device/solution including the details part numbers and Manufacturer's Warranty part number.		
		Bidder must submit the required performance document and feature compliance reference document for the proposed device/solution.		
	Warranty	Mentioning Manufacturer's warranty part number should be quoted, minimum 3 (Three) years warranty should be provided for this unit from the date of commissioning		

Item-26: Wireless Access Point				
SL. #	**Product Names/Items**	**Technical Specifications**	**UOM**	**QTY**
26	**Quality**	ISO 9001/9002 for manufacturer, FCC Class A/B for quality assurance	Set	4
	Brand	To be mentioned by the bidder		
	Model	To be mentioned by the bidder		
	Environmental	Maintain International Quality Environmental Safety Standard		
	Enclosure Type	Ceiling / Wall Mountable		

	Part No	Bidder should submit BOQ of proposed device including the details part numbers. Bidder should submit the required feature & performance compliance document for the proposed solution.		
	Hardware:	Access Points proposed must include radios 2.4 GHz 4dBi and 5 GHz 4dB antennas with 802.11ac Wave 1.		
		Must have an industrial design for durability with steel cases.		
		Mounting kit should be standard from OEM directly.		
		Must have at least 512 MB DRAM and 64 MB flash		
	802.11n & 802.11ac	Must support 4x4 multiple-input multiple-output (MIMO) with three spatial streams		
		Must support simultaneous 802.11n on both the 2.4 GHz and 5 GHz radios.		
		Must support 802.11ac Wave 1 on the integrated 5-GHz radio		
		Must support data rates up to 450Mbps and 1.3 Gbps on 802.11ac.		
		Must support up to 23dbm of transmit power		
	Radio Frequency Features	The Wireless AP should have the technology to improve downlink performance to all mobile devices including one-, two-, and three spatial stream devices on 802.11n and 802.11ac. The technology should work without requiring feedback from clients and should work with all existing 802.11 clients.		
		Should support detecting and classifying non-Wi-Fi wireless transmissions while simultaneously serving network traffic		
		Should support configuring the access point as network connected sensor to access any network location covered by the access point to get real-time Spectrum analysis data.		
		Must support AP enforce load-balance between 2.4Ghz and 5Ghz band		
		Must incorporate radio resource management for power, channel, coverage hole detection and performance optimization		
		Should support spectrum analysis and security scanning using a dedicated hardware separate from the radio serving the clients with 80MHz channel support		
		Must have -100 dB or better Receiver Sensitivity.		
	Network Port	At least 1 x 1GE Ethernet Traffic port and 1 x Console/Management Port		
	Roaming	Must support Proactive Key Caching and/or other methods for Fast Secure Roaming.		
	Security	Must support Management Frame Protection.		
		Should support locally-significant certificates on the APs using a Public Key Infrastructure (PKI).		
		Must operate as a sensor for wireless IPS		
		Should support non-Wi-Fi detection for off-channel rogues and Containment for both radio		
	Encryption	Access Points must support a distributed encryption/decryption model.		
		Access Points must support Hardware-based DTLS encryption on		

		CAPWAP Standard		
	Monitoring	Must support the ability to serve clients and monitor the RF environment concurrently.		
		Same model AP that serves clients must be able to be dedicated to monitoring the RF environment.		
	Flexibility:	AP model proposed must be able to be both a client-serving AP and a monitor-only AP for Intrusion Prevention services.		
		Should support mesh capabilities for temporary connectivity in areas with no Ethernet cabling		
		Mesh support should support QoS for voice over wireless.		
		Must continue serving clients when WAN link to controller is back up again, should not reboot before joining		
		Must support Controller-based and standalone(autonomous) deployments		
		Should support Local authentication at the AP level in case of WAN outage		
	Operational:	Must support telnet and/or SSH login to APs directly for troubleshooting flexibility.		
	Power:	Must support Power over Ethernet, local power(DC Power), and power injectors.		
		Support local power supply unit in future if required		
		Must operate at 3x3 or higher with 802.3af PoE as source of power		
	Quality of Service:	802.11e and WMM		
		Must support Reliable Multicast Video to maintain video quality		
		Must support QoS and Video Call Admission Control capabilities.		
		Access Point should 802.11 DFS certified		
	Design and Implementation Scope	The OEM will prepare the entire design of the BCC Security LAB keeping in mind the compliance requirements and operational requirements.		
		The OEM Validated Design should take into consideration - scalability, modularity, and resiliency aspects of the Security Lab as well as optimization from space, power and cooling perspective.		
		Respective OEM to also ensure that the final deployment is done basis the OEM specified and validated design standards and best practices.		
	Manufacturer's part number	Bidder should submit BOQ of proposed device/solution including the details part numbers and Manufacturer's Warranty part number.		
		Bidder must submit the required performance document and feature compliance reference document for the proposed device/solution.		
	Warranty	Mentioning Manufacturer's warranty part number should be quoted, minimum 3 (Three) years warranty should be provided for this unit from the date of commissioning		

Item-27: Hyper-Visor, VDI & Hyper-Visor Management System				
SL. #	**Product Names/Items**	**Technical Specifications**	**UOM**	**QTY**
27	**Brand**	To be mentioned by the bidder	Lot	1
	Model	To be mentioned by the bidder		
	Part No	Bidder should submit BOQ of proposed device including the details part numbers. Bidder should submit the required feature & performance compliance document for the proposed solution.		
	Product Description	Bidder must propose industry proven, high performance virtualization layer for network service/application virtualization.		
		The Solution should support migration of hyper-visors instance without service disruption to users/application/storage or loss of service/files to schedule downtime for planned maintenance		
		The Solution should support storage backup through deduplication, recovery and replication for DR site / redundant server.		
		The bidder must propose at least 20 units virtual or remote desktops and applications through a VDI and application virtualization platform.		
		The bidder must propose at least 8 CPUs license for hyper-visors and 3 set of central management system for virtual instance create, manage, backup and restore.		
	Design and Implementation Scope	The OEM/Solution Provider will prepare the entire design of the BCC Security LAB keeping in mind the compliance requirements and operational requirements.		
		The OEM/Solution Provider's Validated Design should take into consideration - scalability, modularity, and resiliency aspects of the Security Lab as well as optimization from space, power and cooling perspective.		
		Respective OEM/Solution Provider to also ensure that the final deployment is done basis the OEM/Solution Provider specified and validated design standards and best practices.		
	Manufacturer's part number	Bidder should submit BOQ of proposed device/solution including the details part numbers and Manufacturer's/Solution Provider's Warranty part number.		
		Bidder must submit the required document and feature compliance reference document for the proposed device/solution.		
	Warranty	Mentioning Manufacturer's/Solution Provider's warranty part number should be quoted, minimum 3 (Three) years warranty should be provided for this unit from the date of commissioning		

Item-28: SAN Switch				
SL. #	**Product Names/Items**	**Technical Specifications**	**UOM**	**QTY**
28	**Quality**	ISO 9001/9002 for manufacturer, FCC Class A/B for quality assurance	Set	2
	Brand	To be mentioned by the bidder		
	Model	To be mentioned by the bidder		
	Environmental	Maintain International Quality Environmental Safety Standard		
	Enclosure Type	Rack-mountable Chassis		
	Part No	Bidder should submit BOQ of proposed device including the details part numbers. Bidder should submit the required feature & performance compliance document for the proposed solution.		
	Architecture	The fiber channel switch must be rack mountable. Thereafter, all reference to the 'switch' shall pertain to the 'fiber channel switch'		
		Bidder should propos at least 12 port 16 Gbps FC port switch.		
		The switch must be configured with 12-ports scalable to 48-ports through addition of 16-port incremental port activation license in a 1RU form factor.		
		Bidder should propose 12 x 8 Gbps Fiber Channel short range optical interface for each switch.		
		All 48 x FC ports for device connectivity should be 2/4/8/16 Gbps auto-sensing Fiber Channel ports with dedicated bandwidth per port.		
		The switch must have hot-swappable redundant power supply & fan module without resetting the switch, or affecting the operations of the switch.		
		The switch must be able to support non-disruptive software upgrade.		
		The switch must be able to support Stateful process restart.		
	Storage and Fabric Features	The switch must be capable of creating multiple hardware-based isolated Virtual Fabric (ANSI T11) instances. Each Virtual Fabric instance within the switch should be capable of being zoned like a typical SAN and maintains its own fabric services, zoning database, Name Servers and FSPF processes etc. for added scalability and resilience.		
		The switch must be capable of supporting hardware-based routing between Virtual Fabric instances.		
		The switch must support graceful process restart and shutdown of a Virtual Fabric instance without impacting the operations of other Virtual Fabric instances.		
		The switch shall support hot-swappable Small Form Factor Pluggable (SFP) LC typed transceivers.		
		The switch must support hardware ACL-based Port Security, Virtual SANs (VSANs), and Port Zoning.		
		The switch must support Smart Zoning such that the entries in the TCAM are significantly reduced and therefore increasing the overall scalability of the SAN Fabric.		

		Inter-switch links must support the transport of multiple Virtual Fabrics between switches, whilst preserving the security between Virtual Fabrics.		
		The switch must support routing between Virtual Fabric instances in hardware.		
		The switch shall support FC-SP for host-to-switch and switch-to-switch authentication.		
		The switch must support the following fabric services:		
		Name server		
		Registered State Change Notification (RSCN)		
		Login services		
		Public loop		
		Broadcast		
		In-order delivery		
		Name server zoning		
		The switch must comply with the following FC standards: -		
		FC-PH-3, Revision 9.4		
		FC-GS-3, Revision 7.01		
		FC-FLA, Revision 2.7		
		FC-SW-2, Revision 5.3		
		FC-VI, Revision 1.61		
		FCP-2, Revision 7		
		FC-SB-2, Revision 2.1		
		IP over Fiber Channel (RFC 2625)		
		Extensive IETF-standards-based TCP/IP, SNMPv3, and Remote Monitoring (RMON) MIBs		
		Class of service: Class 2, Class 3, Class F		
		Fiber Channel standard port types: E, F, FL		
		Fiber Channel enhanced port types: SD, TE		
		The switch must support port mirroring for both Fiber Channel and Gigabit Ethernet (802.3z), such that traffic going to a specific port can be mirrored and forwarded to another port for analyzing.		
		The switch must be able to immediately recover in the event of a failed forwarding path going via an alternative path.		
		The switch must also support load balancing across multiple paths through the fabric via Fabric Shortest Path First (FSPF).		
		Using FSPF, the switch must be able to load balance up to 16 equal cost paths across the SAN network.		
		The switch must be able to support port aggregation of up to 16 physical Fibre Channel ports into a single aggregated link. The aggregated ports must NOT be consecutive ports on a line card.		
		The switch must support the aggregation of any ports from any module.		

		The switch must be able to load balance traffic through an aggregated link with Source ID and Destination ID. The support for load balancing utilizing the Exchange ID must also be supported.		
		The switch must be equipped with congestion control mechanisms such that it is able to throttle back traffic away from a congested link.		
		The switch must be capable of discovering neighboring switches and identify the neighboring Fiber Channel or Ethernet switches.		
	Security Features	The switch must support RADIUS authentication when managing from GUI, console or telnet to prevent unauthorized access		
		The switch must support Secure Shell (SSH) encryption to provide additional security for Telnet sessions to the switch.		
		The switch must support multilevel security on console access prevents unauthorized users from altering the switch configuration.		
		The switch must support role-based administration by allowing different administrators different access rights to the switch. Role-based access control will use RADIUS or AAA functions.		
		The switch must support SNMPv3 for secured management.		
	High-Availability	Hot-swappable, dual redundant power supplies		
		Hot-swappable fan tray		
		Hot-swappable SFP+ optics		
		In Service Software Upgrade (ISSU) or similar mechanism		
		Stateful process/feature restart		
	Management and Troubleshooting Features	The switch shall support the following Management Access Control		
		SSHv2		
		SNMPv3		
		IP ACLs		
		Switch must support Fiber Channel Traceroute and Fiber Channel Ping for ease of troubleshooting and fault isolation. In addition, the switch must also support the following diagnostics.		
		Diagnostics tool		
		Loopbacks		
		Storage Fabric Analyzing		
		SPAN		
		FC Debugging		
		Syslog		
		Port level statistics		
		Switch must support out-band management protocols like SNMP, SNMPv3, SMI-S, Telnet, FTP and TFTP.		
		The switch should support IPv6.		
	Design and Implementation Scope	The OEM will prepare the entire design of the BCC Security LAB keeping in mind the compliance requirements and operational requirements.		

		The OEM Validated Design should take into consideration - scalability, modularity, and resiliency aspects of the Security Lab as well as optimization from space, power and cooling perspective.		
		Respective OEM to also ensure that the final deployment is done basis the OEM specified and validated design standards and best practices.		
	Manufacturer's part number	Bidder should submit BOQ of proposed device/solution including the details part numbers and Manufacturer's Warranty part number.		
		Bidder must submit the required performance document and feature compliance reference document for the proposed device/solution.		
	Warranty	Mentioning Manufacturer's warranty part number should be quoted, minimum 3 (Three) years warranty should be provided for this unit from the date of commissioning		

Item – 29: Storage Server

SL. #	Product Names/Items	Technical Specifications	UOM	QTY
29	**Quality**	ISO 9001/9002 for manufacturer, FCC Class A/B for quality assurance	Set	1
	Brand	To be mentioned by the bidder		
	Model	To be mentioned by the bidder		
	Environmental	Maintain International Quality Environmental Safety Standard		
	Enclosure Type	Rack-mountable Chassis		
	Part No	Bidder should submit BOQ of proposed device including the details part numbers. Bidder should submit the required feature & performance compliance document for the proposed solution.		
	CPU Cores	2 x Intel E5-2667 v4 3.20 GHz Processor or higher model		
	Cache Memory	Min 25 MB Cache per processor or higher		
	Chipset	Intel C610 series chipset or higher		
	Memory	Min. 24 slots for ECC DIMMs or higher		
		Min. 256 GB DDR4-2400-MHz RDIMM RAM with Advanced error-correcting code (ECC).		
		Support for advanced memory redundant technologies like Advanced error-correcting code (ECC) and memory mirroring / Mirrored Memory		
		Expandable minimum 768 GB Memory		
	Interconnect	2 Intel Quick Path Interconnect (QPI) channels with 6.4 GT per second, 8.0 GT per second and 9.6 GT per second.		
	RAID Controller	12 Gbps SAS modular RAID controller, RAID JBOD, RAID 0, 1, 10, 5, 6, 50, and 60.		
		RAID card should support at least 24 Hard Drive to enable RAID functionality with 2 GB Cache		
		The modular RAID controller should be upgradable up to 4Gb cache in future if required with JBOD, RAID 0, 1, 10, 5, 6, 50, and 60.		
	Hard Disk Drives	12 x 4 TB 12Gb SAS 7.2K RPM Hard-Disk for each server		

		1 x 120 GB 2.5-inch Enterprise grade 6Gb SATA SSD Hard-Disk for each server		
		All the bay should support SAS or SATA hard drives (HDDs) or solid state drives (SSD)		
	Optical Drive	DVD + /-RW Drive integrated/external or Virtual media support for remote CD and DVD drives		
	Expansion Slots	Min. 6 PCI-Express Generation 3 slots		
	I/O Ports	Min. 1 USB 3.0 ports, 1 Serial port, 1 VGA ports		
	USB/Flash Drive	Must have an internal slot for SD card / Flash which supports booting hypervisors.		
	Ethernet Port	6 x 1000Mbps Ethernet ports with below feature enabled		
		Pre-Execution Boot (PXE boot)		
		iSCSI boot		
		Checksum and segmentation offload		
		NIC teaming		
		2 x 8G Fiber Channel HBA ports		
		Must have at least one PICE slot for 1 , 10 or 40 GbE network connectivity for future scalability.		
		The server should support the capability to use up to 40-Gbps unified network fabric which aggregates both the Ethernet and FC connectivity on a single controller using Low-latency, lossless, 10-Gbps Ethernet and industry-standard Fibre Channel over Ethernet (FCoE) fabric		
		Dedicated one Gigabit Ethernet management port		
	Power Supply	Dual Redundant Hot-plug, AC Power Supply		
	Fan Module	Hot-swappable fans module		
	Accessories	Rail Kit and Cable management should be offered		
	Storage Operating System	Bidder must propose software based storage system which can perform both 8Gbp and 16 Gbps FC protocols with storage data management.		
	Systems Management	Web user interface for server management; remote keyboard, video, and mouse (KVM), virtual media and administration		
		The server should support Intelligent Platform Management Interface (IPMI) 2.0 support for out-of-band management through third-party enterprise management systems		
		Should capable to view server properties and sensors		
		Should capable to monitor faults, alarms, and server status		
		Should capable to power on, power off, power cycle, reset, and shut down the server		
		Out-of-band management		
		wake-on-LAN (WoL)		
		Command-line interface (CLI)		
	Environmental Requirement	Operating Temperature support from 5° Celsius to 35° Celsius and non-operation Temperature from -40° Celsius to 65 °Celsius.		

		Operating Humidity from 10 to 90% non-condensing temperature		
		Operating Altitude from 0 to 2950 meter and Non-operating Altitude from 0 to 11,900 meter		
	Design and Implementation Scope	The OEM will prepare the entire design of the BCC Security LAB keeping in mind the compliance requirements and operational requirements.		
		The OEM Validated Design should take into consideration - scalability, modularity, and resiliency aspects of the Security Lab as well as optimization from space, power and cooling perspective.		
		Respective OEM to also ensure that the final deployment is done basis the OEM specified and validated design standards and best practices.		
	Manufacturer's part number	Bidder should submit BOQ of proposed device/solution including the details part numbers and Manufacturer's Warranty part number.		
		Bidder must submit the required performance document and feature compliance reference document for the proposed device/solution.		
	Warranty	Mentioning Manufacturer's warranty part number should be quoted, minimum 3 (Three) years warranty should be provided for this unit from the date of commissioning		

Item-30:Firewall (Type-1)				
SL. #	**Product Names/Items**	**Technical Specifications**	**UOM**	**QTY**
30	**Quality**	ISO 9001/9002 for manufacturer, FCC Class A/B for quality assurance	Set	1
	Brand	To be mentioned by the bidder		
	Model	To be mentioned by the bidder		
	Environmental	Maintain International Quality Environmental Safety Standard		
	Enclosure Type	Rack-mountable Chassis		
	Part No	Bidder should submit BOQ of proposed device including the details part numbers. Bidder should submit the required feature & performance compliance document for the proposed solution.		
	Hardware Architecture	The appliance based security platform should be capable of providing firewall, application visibility, and IPS functionality in a single appliance. The solution should support next-generation firewall from day 1 and IPS & malware protection with application visibility/identification will be enabled in future if required.		
		Proposed solution should be dedicated firewall appliance and should not be a subset of Router or UTM.		
		The appliance should support at least 8 x 1G and should be scalable to additional 6 x 1G ports in future		
		The appliance hardware should be multi-core CPU architecture with a hardened 64 bit operating system to support higher memory.		
		Proposed Firewall should not be proprietary ASIC based in nature & should be open architecture based on multi-core CPS's to protect & scale against dynamic latest security threats.		

	Performance & Scalability	Should support at least 1.8 Gbps of Stateful inspection throughput with multiprotocol/IMIX/Real-world HTTP traffic.		
		Should support at least 1.2 Gbps of NGFW performance throughput (includes FW, Application Visibility & IPS)		
		NG Firewall should support at least 1000,000 concurrent sessions		
		NG Firewall should support at least 50,000 connections per second with Application visibility		
		NG Firewall should support at least 200 VLANs		
		Should support at least 10 firewall context/virtual firewall system (VSYS) context with separate management and traffic separation from day 1 and it can be scaled up at least 90 in future if required.		
	High-Availability Features	Firewall should support Active/Standby or Active-Active failover		
		Firewall should support ether channel functionality for the failover control & date interfaces for provide additional level of redundancy		
		Firewall should support redundant interfaces to provide interface level redundancy before device failover		
		Firewall should support 802.3ad Ether channel functionality to increase the bandwidth for a segment.		
		Firewall should have integrated redundant power supply		
	NGFW Features	Should support the capability of passively gathering information about network hosts and their activities, such as operating system, services, open ports, client applications, and vulnerabilities, to assist with multiple activities, such as intrusion event data correlation, elimination of false positives, and policy compliance.		
		Firewall should support creating access-rules with IPv4 & IPv6 objects simultaneously		
		Firewall should support operating in routed & transparent mode		
		Should support Static, RIP, OSPF, OSPFv3 and BGP, BGPv6		
		Firewall should support manual NAT and Auto-NAT, static Nat, dynamic Nat, dynamic pat		
		Firewall should support Nat66 (IPv6-to-IPv6), Nat 64 (IPv6-to-IPv4) & Nat46 (IPv4-to-IPv6) functionality		
		Firewall should support Multicast protocols like IGMP, PIM, etc		
		Should support security policies based on security group names in source or destination fields or both, Network, Application, user, geo location		
		Should support the capability of dynamically tuning IDS/IPS sensors (e.g., selecting rules, configuring policies, updating policies, etc.) with minimal human intervention.		
		Should support the capability of automatically providing the appropriate inspections and protections for traffic sent over non-standard communications ports.		
		Should be able to link Active Directory and/or LDAP usernames to IP addresses related to suspected security events.		
		Should be capable of detecting and blocking IPv6 attacks.		
		Should support the capability to quarantine end point		

		Solution should support full-featured NBA capability to detect threats emerging from inside the network. This includes the ability to establish “normal” traffic baselines through flow analysis techniques (e.g., NetFlow) and the ability to detect deviations from normal baselines.		
		Should support to provide IP reputation feed that comprised of several regularly updated collections of poor reputation of IP addresses determined by the proposed security vendor		
		Solution support IP reputation intelligence feeds from third party and custom lists of IP addresses including a global blacklist.		
		Should support URL and DNS threat intelligence feeds to protect against threats		
		Should support Reputation- and category-based URL filtering offering comprehensive alerting and control over suspect web traffic and enforces policies on more than 275 million of URLs in more than 80 categories.		
		Should support safe search and YouTube EDU enforcement		
		Solution must be capable of passively gathering details unique to mobile devices traffic to identify a wide variety of mobile operating systems, mobile applications and associated mobile device hardware.		
		Should support more than 3900 application layer and risk-based controls that can invoke tailored intrusion prevention system (IPS) threat detection policies to optimize security effectiveness.		
		Should support capability of providing network-based detection of malware by checking the disposition of known files in the cloud using the SHA-256 file-hash as they transit the network and capability to do dynamic analysis on-premise on purpose built-appliance (if required in future)		
		NGFW OEM must have its own threat intelligence analysis center and should use the global footprint of security deployments for more comprehensive network protection.		
		The detection engine should support capability of detecting and preventing a wide variety of threats (e.g., malware, network probes/reconnaissance, VoIP attacks, buffer overflows, P2P attacks, etc.).		
		Should support the ability to identify attacks based on Geo-location and define policy to block on the basis of Geo-location		
		The detection engine should support the capability of detecting variants of known threats, as well as new threats		
		The detection engine must incorporate multiple approaches for detecting threats, including at a minimum exploit-based signatures, vulnerability-based rules, protocol anomaly detection, and behavioral anomaly detection techniques. Identify and explain each type of detection mechanism supported.		
		Should support Open based Application ID for access to community resources and ability to easily customize security to address new and specific threats and applications quickly		
	Management	The management platform must be accessible via a web-based interface and ideally with no need for additional client software		
		The management platform must provide a highly customizable		

		dashboard.		
		The management platform must be capable of integrating third party vulnerability information into threat policy adjustment routines and automated tuning workflows		
		The management platform must be capable of role-based administration, enabling different sets of views and configuration capabilities for different administrators subsequent to their authentication.		
		Should support REST API for monitoring and configuration programmability		
		The management platform must provide multiple report output types or formats, such as PDF, HTML, and CSV.		
		The management platform must support multiple mechanisms for issuing alerts (e.g., SNMP, e-mail, SYSLOG).		
		The management platform must provide robust reporting capabilities, including a selection of pre-defined reports and the ability for complete customization and generation of new reports.		
		The management platform must risk reports like advanced malware, attacks and network		
		The management platform must include an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to enable events and log data to be shared with external network and security management applications, such as Security Information and Event Managers (SIEMs), and log management tools.		
	Design and Implementation Scope	The OEM will prepare the entire design of the BCC Security LAB keeping in mind the compliance requirements and operational requirements.		
		The OEM Validated Design should take into consideration - scalability, modularity, and resiliency aspects of the Security Lab as well as optimization from space, power and cooling perspective.		
		Respective OEM to also ensure that the final deployment is done basis the OEM specified and validated design standards and best practices.		
	Manufacturer's part number	Bidder should submit BOQ of proposed device/solution including the details part numbers and Manufacturer's Warranty part number.		
		Bidder must submit the required performance document and feature compliance reference document for the proposed device/solution.		
	Warranty	Mentioning Manufacturer's warranty part number should be quoted, minimum 3 (Three) years warranty should be provided for this unit from the date of commissioning		

Item-31:Firewall (Type-2)				
SL. #	**Product Names/Items**	**Technical Specifications**	**UOM**	**QTY**
31	**Quality**	ISO 9001/9002 for manufacturer, FCC Class A/B for quality assurance	Set	1
	Brand	To be mentioned by the bidder		
	Model	To be mentioned by the bidder		
	Environmental	Maintain International Quality Environmental Safety Standard		

	Enclosure Type	Rack-mountable Chassis		
	Part No	Bidder should submit BOQ of proposed device including the details part numbers. Bidder should submit the required feature & performance compliance document for the proposed solution.		
	Hardware Architecture	The appliance based security platform should be capable of providing firewall functionality in a single appliance		
		The appliance hardware should be a multi-core CPU architecture with a hardened 64 bit operating system to support higher memory		
		Proposed Firewall should not be proprietary ASIC based in nature & should be open architecture based on multi-core CPU to protect & scale against dynamic latest security threats.		
		Should have minimum 6 GB System Memory and minimum 6 GB Flash Memory		
	Interface Requirement	Firewall device should have at least 6 x 1GE interfaces as Traffic interface from day 1.		
		Firewall device should have one expansion module slot for future expansion		
		Firewall can be upgraded to minimum 14 ports 1GE interfaces in future		
		Expansion Interface module should support optical Gigabit Ethernet interfaces.		
		Should have 1 console and auxiliary port.		
	Firewall Performance	Minimum 1.9 Gbps Firewall Stateful inspection throughput		
		Minimum 950 Mbps Firewall Stateful inspection throughput with multi-protocol traffic		
		Should support minimum 620 Mbps Next-Generation (NG) firewall		
		3DES VPN performance should be minimum 290 Mbps		
		Firewall should support minimum vlans 195		
		IPSec VPN peers minimum >= 720		
		Minimum concurrent connection >= 490,000 (490K)		
		Minimum New Connections/Second >= 19,000 (19K)		
		Support for Jumbo frames of up to 9000 bytes		
		Minimum 2 Security Contexts/virtual firewall (VSYS) with separate management & control plan and it can be upgradable up to 20 in future if required.		
	High-Availability Features	Firewall should support Active/Standby or Active-Active failover		
		Firewall should support ether channel/ lacp functionality for the failover control & date interfaces for provide additional level of redundancy		
		Firewall should support redundant interfaces to provide interface level redundancy before device failover		
		Firewall should support 802.3ad Ether channel/lacp functionality to increase the bandwidth for a segment.		
	Firewall Features	The Firewall should support transparent (Layer 2) firewall or routed (Layer 3) firewall operation		

		Support Ether Channel / Link Aggregation Protocol for Link Failure protection		
		Firewall should support static NAT, Policy based NAT and PAT		
		Firewall should support IPSec data encryption		
		Firewall should support client based IPSec VPN Tunnels		
		Firewall should support IPSec NAT Traversal		
		Support for Standard Access Lists and Extended Access Lists to provide supervision and control.		
		Control SNMP access through the use of SNMP with MD5 authentication.		
		Implement Access Lists on the router to ensure SNMP access only to the SNMP manager or the NMS workstation.		
		Support Multiple Privilege Levels for access.		
		Support for Remote Authentication Dial-In User Service (RADIUS) and AAA or similar protocol		
	Management Features	Support for Central Management Software for simple, secure remote management through Web-based GUI.		
		Should provide a wide range of informative, real-time, and historical reports that give critical insight into usage trends, performance baselines, and security events.		
		Support accessible through variety of methods, including console port, Telnet, and SSHv2.		
		Ability to generate AAA records for tracking administrative access to appliances, as well as tracking all configuration changes made during an administrative session.		
		Support for SNMPv2 providing in-depth visibility into the status of appliances.		
		Support accurate time stamping and numbering of Syslog messages while supporting multiple Syslog servers over either TCP or UDP as the transport protocol.		
		Should capable to perform configuration rollback and offers the ability to store and use multiple configurations and software images in compact flash memory.		
		Support prevention of unauthorized access to sensitive configuration data, certificates, and key material stored on the security appliance by automatically wiping flash memory contents if an asset recovery or password reset procedure occurs.		
		Support a convenient method for alerting administrators when critical events are encountered, by sending e-mail alert messages to administrator defined e-mail addresses.		
	Design and Implementation Scope	The OEM will prepare the entire design of the BCC Security LAB keeping in mind the compliance requirements and operational requirements.		
		The OEM Validated Design should take into consideration - scalability, modularity, and resiliency aspects of the Security Lab as well as optimization from space, power and cooling perspective.		
		Respective OEM to also ensure that the final deployment is done basis the OEM specified and validated design standards and best practices.		

	Manufacturer's part number	Bidder should submit BOQ of proposed device/solution including the details part numbers and Manufacturer's Warranty part number.		
		Bidder must submit the required performance document and feature compliance reference document for the proposed device/solution.		
	Warranty	Mentioning Manufacturer's warranty part number should be quoted, minimum 3 (Three) years warranty should be provided for this unit from the date of commissioning		

Item-32: SIEM and Data Analytics System				
SL. #.	**Product Names/Items**	**Technical Specifications**	**UoM**	**QTY**
32	**Quality**	ISO 9001/9002 for manufacturer, FCC Class A/B for quality assurance	Lot	1
	Brand	To be mentioned by the bidder		
	Model	To be mentioned by the bidder		
	Part No	Bidder should submit BOQ of proposed device including the details part numbers. Bidder should submit the required feature & performance compliance document for the proposed solution.		
	SIEM & Data Analytics System Generic Requirement	The solution should capable to search, report, monitor and analyze historical data across network infrastructure in real time with user transaction log, user behavior pattern, machine/device behavior pattern, security threats and fraudulent activity.		
		The solution should have at least 10Gb data indexing volume per day.		
		The solution should have step-by-step/wizard based process workflow to simplify on boarding of any data source.		
		The solution should have real-time indexing of machine/device data		
		The solution should have searching capability throughout real-time data and historical data.		
		The solution should have searching capability on multiple software deployments. It also supports load balancing feature and failover/redundancy.		
		The solution should monitor and alert for individual events and correlated real time events.		
		The solution should support reports across real-time and historical data		
		The solution should support knowledge mapping feature for machine data objects		
		The solution should support customizable and collaborative dashboards integrating real-time machine data, tables, charts and reports.		
		The solution should support data/log modeling for consistent relationships in machine/device data		
		The solution should support drag and drop to customize, discover and visualize machine/device data.		
		The solution should discover patterns and similarities in data/log automatically with command/click.		
		The solution should have high performance analytical functionality.		
		The solution should have transparent report/data summarization functionality.		

		The solution should have charts and reports for other third-party business applications.		
		The solution should have scheduling and automatic generation and delivery of reports.		
		The solution should have role based access control (RBAC) and user authentication with LDAP/RADIUS/directory and single sign-on features.		
		The solution should have high availability active-active/active-standby/clustering architecture for data availability in central site and disaster recovery as multisite deployment with centrally management of distributed deployments.		
		The solution should support monitoring and deploying data/log forwarder configurations, secure and reliable data/log forwarding from remote site to central site in real time.		
		Support developing SDK/Interface for building application with web programming.		
		The propose solution should have support with full Access product documentation, application, support forum.		
		The propose solution should have access for support portal, ability to manage cases online, tailored support levels or support escalation.		
	Design and Implementation Scope	The OEM/Solution Provider will prepare the entire design of the BCC Security LAB keeping in mind the compliance requirements and operational requirements.		
		The OEM/Solution Provider's Validated Design should take into consideration - scalability, modularity, and resiliency aspects of the Security Lab as well as optimization from space, power and cooling perspective.		
		Respective OEM/Solution Provider to also ensure that the final deployment is done basis the OEM/Solution Provider specified and validated design standards and best practices.		
	Manufacturer's part number	Bidder should submit BOQ of proposed device/solution including the details part numbers and Manufacturer's/Solution Provider's Warranty part number.		
		Bidder must submit the required document and feature compliance reference document for the proposed device/solution.		
	Warranty	Mentioning Manufacturer's/Solution Provider's warranty part number should be quoted, minimum 3 (Three) years warranty should be provided for this unit from the date of commissioning		

Item-33: Industrial Switch (Type-1)				
SL. #	**Product Name/Items**	**Technical Specifications**	**UOM**	**QTY**
33	**Quality**	ISO 9001/9002 for manufacturer, FCC Class A/B for quality assurance	Set	1
	Brand	To be mentioned by the bidder		
	Model	To be mentioned by the bidder		
	Environmental	Maintain International Quality Environmental Safety standard		
	Enclosure Type	Rack Mountable with Rack Mounting Kit		
	Part No	Bidder should submit BOQ of proposed device including the details part numbers. Bidder should submit the required feature & performance compliance document for the proposed solution.		
	Switch Architecture	Bidder should propose at least 12 port 10/100/1000BaseT PoE/PoE+ Ports, 12 Port 100/1000Base-X Optical Port and 4 port SFP as uplink port with 3 x 1GE SX Module. All the SFP should be OEM Original Module		
		The switch should be industrial grade by hardened for vibration, shock, surge, and electrical noise immunity.		
		The switch should be without fans, convection cooling architecture for longer durability and operation.		
		The switch should have crystal oscillator to provide highest frequency stability for accurate synchronization applications.		
		The switch should built for Supervisory Control And Data Acquisition (SCADA) network.		
		The switch must have dual power supply.		
	Switch Performance	The switch should have at least 26Gbps Forwarding Bandwidth		
		The switch should have at least 52Gbps Switching Bandwidth		
		The switch should have at least 40 Mpps Switching Bandwidth		
		The switch should have at least 15,000 MAC Address		
		The switch should have at least 1,000 IPv4 MAC security entries		
		The switch should have at least 250 unique IP subnet NAT translation entries		
	Layer 2 Features	IEEE 802.1, 802.3, 802.3at, 802.3af standard, NTP, UDLD, CDP, LLDP, Unicast Mac filter, Resilient Ethernet Protocol (REP), Ether Channel/lacp, Voice VLAN, QinQ tunneling, Media Redundancy Protocol (MRP/IEC 62439-2)		
		IGMPv1, v2, v3 Snooping, IGMP filtering		
		IPv6 Host support, HTTP over IPv6, SNMP over IPv6		
		Layer 2 switching with 1:1 static Network Address Translation (NAT)		
	Layer 3 Features	IPv4 Static Routing		
		OSPF, BGPv4, IS-IS, RIPv2, RIPng, OSPFv6		

		PIM sparse mode (PIM-SM), PIM dense mode (PIM-DM), and PIM sparse-dense mode		
		VRF-Lite		
	Network Security Features	SSH, SNMPv3, RADIUS Server/Client, MAC Address Notification, Storm Control for Unicast, Multicast, Broadcast		
		BPDU Guard, Port -Security, Private VLAN, DHCP Snooping, Dynamic ARP Inspection, IP Source Guard		
		802.1x, Guest VLAN, MAC Authentication Bypass, 802.1x Multi-Domain Authentication		
		IEEE 802.1AE MACSec		
	Quality of Service (QoS) & Control	Ingress Policing, Rate-Limit		
		Egress Queuing/shaping		
		Automatic QoS or similar protocol		
		Modular QoS command line or similar technology		
	Standards & Compliance	IEEE 1588 v2 PTP Power Profile, dying gasp, GOOSE messaging, SCADA protocol classification, MODBUS TCP/IP, utility Smart Port macro, BFD, Ethernet OAM, IEEE 802.3ah, CFM (IEEE 802.1ag)		
		IRIG-B Output interface (B002, B003, B006, B007, B122, B123, B126, B127 time code)		
		CIP Ethernet/IP, Profi-net v2, IEEE 1588 PTP v2 Default Profile, CIP Time Sync, NTP to PTP Translation		
		EN 61000-6-1 Immunity for Light Industrial Environments, EN 61000-6-2 Immunity for Industrial Environments EN 61326 Industrial Control, EN 61131-2 Programmable Controllers IEEE 1613 Class 2 Electric Power Stations Communications Networking, IEC 61850-3 Electric Substations Communications Networking EN50155 Railway - Electronic Equipment on Rolling Stock (EMC, ENV, Mech) EN50121-4 Railway - Signaling and Telecommunications Apparatus EN50121-3-2 Railway - Apparatus for Rolling Stock ODVA Industrial Ethernet/IP PROFINET conformance B IP30 (per EN60529)		
	Management	Web Based Configuration Manager, MIB, SNMP, Syslog, SPAN Sessions, RSPAN, DHCP Server, digital optical management or similar protocol, hardware watchdog or similar mechanism, Industrial Network Director, Netflow Lite or similar protocol		
	Design and Implementation Scope	The OEM will prepare the entire design of the BCC Security LAB keeping in mind the compliance requirements and operational requirements.		
		The OEM Validated Design should take into consideration - scalability, modularity, and resiliency aspects of the Security Lab as well as optimization from space, power and cooling perspective.		
		Respective OEM to also ensure that the final deployment is done basis the OEM specified and validated design standards and best practices.		
	Manufacturer's part number	Bidder should submit BOQ of proposed device/solution including the details part numbers and Manufacturer's Warranty part number.		

		Bidder must submit the required performance document and feature compliance reference document for the proposed device/solution.		
	Warranty	Manufacturer's warranty part number should be mentioned, minimum 3 (Three) years warranty should be provided for this unit from the date of commissioning		

Item-34: Industrial Switch (Type-2)				
SL. #	**Product Name/Items**	**Technical Specifications**	**UOM**	**QTY**
34	**Quality**	ISO 9001/9002 for manufacturer, FCC Class A/B for quality assurance	Set	1
	Brand	To be mentioned by the bidder		
	Model	To be mentioned by the bidder		
	Environmental	Maintain International Quality Environmental Safety standard		
	Enclosure Type	Rack Mountable with Rack Mounting Kit		
	Part No	Bidder should submit BOQ of proposed device including the details part numbers. Bidder should submit the required feature & performance compliance document for the proposed solution.		
	Switch Architecture	Bidder should propose 8 x 10/100 BaseT Ethernet ports and 2 SFP either 10/100/1000 copper or SFP fiber port as uplinks		
		The switch should have at least two expansion modules for port expansion		
		The switch should be built for Industrial Ethernet applications where extreme environmental like heat/smoke/dust, shock/vibration environment, surge ratings and convection cooling.		
		The switch must have AC power supply from day 1.		
	Switch Performance	The switch should have at least 16 Gbps switching fabric for non-blocking/wire-speed switching capacity		
		The switch should have at least 6 Mpps Forwarding rate based on 64-byte packets		
		The switch should have at least 8000 MAC addresses for Layer 2		
		The switch should have at least 250 IGMP multicast groups		
		Support Jumbo frames at least 9018 bytes on uplink ports		
		Support MTU at least 1998 bytes		
	Layer 2 Features	VLAN, 802.1q trunking		
		Resilient Ethernet Protocol (REP)		
		IEEE 802.1d Spanning Tree Protocol		
		Ether Channel /LACP		
	Layer 3 Features	The switch should have at least 3,000 unicast routes		
		L3 VLAN, RIPv1, RIPv2 and RIPng, OSPF, IS-IS, BGPv4, OSPFv6		
		The switch should have at least 1000 multicast groups		
		VRF-Lite		

	Network Security Features	IEEE 802.1x, Port-based ACLs, MAC address filtering, MAC address notification, Port security		
		IGMP filtering, Per-port broadcast, multicast, and unicast storm control		
		Secure Shell (SSH) Protocol v2, SNMPv3		
		Dynamic Host Configuration Protocol (DHCP) snooping, DHCP Interface Tracker (Option 82)		
		RADIUS authentication, standard and advance IP security ACLS, Dynamic ARP Inspection, IP source guard, private VLAN, IGMPv3 snooping		
		The switch must have at least 350 security ACLs		
	Quality of Service (QoS) & Control	QoS classification and prioritization for mission-critical data		
		The switch must have at least 125 QoS policies		
	Standards & Compliance	IEC61850 and IEEE1613, NEMA TS-2, PROFINET v2, PROFINET conformance class B, IEEE1588v2,		
		Standard for Industrial Ethernet specifications like industrial automation, ITS, substation, railway applications,		
	Management	SNMP v1/v2/v3		
	Design and Implementation Scope	The OEM will prepare the entire design of the BCC Security LAB keeping in mind the compliance requirements and operational requirements.		
		The OEM Validated Design should take into consideration - scalability, modularity, and resiliency aspects of the Security Lab as well as optimization from space, power and cooling perspective.		
		Respective OEM to also ensure that the final deployment is done basis the OEM specified and validated design standards and best practices.		
	Manufacturer's part number	Bidder should submit BOQ of proposed device/solution including the details part numbers and Manufacturer's Warranty part number.		
		Bidder must submit the required performance document and feature compliance reference document for the proposed device/solution.		
	Warranty	Manufacturer's warranty part number should be mentioned, minimum 3 (Three) years warranty should be provided for this unit from the date of commissioning		

Item-35: Industrial Router				
SL. #	**Product Name/Items**	**Technical Specifications**	**UOM**	**QTY**
35	**Quality**	ISO 9001/9002 for manufacturer, FCC Class A/B for quality assurance		2
	Brand	To be mentioned by the bidder		
	Model	To be mentioned by the bidder		
	Environmental	Maintain International Quality Environmental Safety standard		
	Enclosure Type	Rack Mountable with Rack Mounting Kit		

	Part No	Bidder should submit BOQ of proposed device including the details part numbers. Bidder should submit the required feature & performance compliance document for the proposed solution.		
	Router Architecture	The router should have advanced data routing, firewall, traffic shaping, quality of service, and network segmentation feature.		
		The router must be IEEE 1613 and IEC 61850-3 substation standards for ruggedizing with convection cooling, EMI and surge protection.		
		The router should be Industrial-grade modular architecture with modular interfaces and hot-swappable power supplies.		
		The switch must have AC power supply from day 1.		
	Interface Requirement	The router should have at least two Gigabit Ethernet WAN interfaces, supporting two GE Fiber or two GE Copper.		
		Bidder should propose 1 x 1GE Multi-Mode SFP for each Router.		
		The router should support T1/E1, 8-port asynchronous /synchronous /RS-232 serial interfaces.		
	Protocol & Encapsulations Support	The router should support Dynamic Multipoint VPN, Firewall, Intrusion Prevention System, Content Filtering, Packet Matching, public key infrastructure (PKI) and AAA.		
		The router should support IP SLA or similar mechanism		
		The router should support Netflow		
		The router should support QoS, ACLS etc.		
		The router should support IPv4, IPv6, static routes, Open Shortest Path First (OSPF), , Border Gateway Protocol (BGP), BGP Router Reflector, Intermediate System-to-Intermediate System (IS-IS), Multicast Internet Group Management Protocol (IGMPv3), Protocol Independent Multicast sparse mode (PIM SM), PIM Source Specific Multicast (SSM), IPSec, Generic Routing Encapsulation (GRE), Bi-Directional Forwarding Detection (BVD), IPv4-to-IPv6 Multicast, MPLS, L2TPv3, IEEE 802.1ag, IEEE 802.3ah, and L2 and L3 VPN		
		The router should support Ethernet, IEEE 802.1q VLAN, Point-to-Point Protocol (PPP), Multilink Point-to-Point Protocol (MLPPP), Frame Relay, Multilink Frame Relay (MLFR) , Serial (RS-232), Point-to-Point Protocol over Ethernet (PPPoE), and ATM, DNP3, and MODBUS SCADA Tunneling (BSTUN)		
		The router should have hardware based encryption engine for IPSec and SSL.		
	High-Availability	Support Hot-standby capabilities in redundant router installation /configuration.		
		Support Bidirectional Forwarding Detection		
		Support dual power supply.		
	Management	Simple Network Management Protocol (SNMP) , Syslog		
		SSH, Telnet, Remote Monitoring (RMON), NetFlow, and TR-069		
	Design and Implementation	The OEM will prepare the entire design of the BCC Security LAB keeping in mind the compliance requirements and		

	Scope	operational requirements.		
		The OEM Validated Design should take into consideration - scalability, modularity, and resiliency aspects of the Security Lab as well as optimization from space, power and cooling perspective.		
		Respective OEM to also ensure that the final deployment is done basis the OEM specified and validated design standards and best practices.		
	Manufacturer's part number	Bidder should submit BOQ of proposed device/solution including the details part numbers and Manufacturer's Warranty part number.		
		Bidder must submit the required performance document and feature compliance reference document for the proposed device/solution.		
	Warranty	Manufacturer's warranty part number should be mentioned, minimum 3 (Three) years warranty should be provided for this unit from the date of commissioning		

Item-36: Training Platform Module				
SL. #.	**Product Names/Items**	**Description of requirements**	**UoM**	**QTY**
	Solution name:	Training Platform Module encompasses Cyber Attack Simulation functionalities.		
1	**Classroom management**	Should allow to manage centrally workstations with the following futures:	Set	1
	Centralized software management	Remotely deploy, execute, and control software on windows based managed workstations		
	Snapshot	Snapshot of operating system and its configuration and reverting upon special remote command execution		
	Preventing unauthorized access	Prevent unauthorized administrators from accessing or controlling a computer		
2	**Monitoring**	To install, configure and maintain distributed monitoring solution with the following futures:	Set	1
	Deployment	Deployment to selected VM located in Server		
	Permissions management	Secure user authentication and availability to limit accessibility to components for authenticated users		
	Data gathering	Availability checks, performance checks, SNMP (both trapping and polling), IPMI, JMX, VMware monitoring, custom checks, gathering data at custom intervals. Both modes: server/proxy mode or by agents Ability to gather data from Linux and Windows machines, including binary daemons Ability to track activity of MODBUS protocol		
	Data storing and API	Gathered data should be stored in a database and be accessible through API for Automated scoring system module		
	Alerting	Customisable notifications (by email and in application) with ability to use macro variables. Ability to configure semi-automated and automated management actions, including execution of remote commands		
	Real-time data representation in visual format	Monitored items should be immediately displayed in visuals located in Command and control center module and Automated scoring system module Custom graphs, network maps, custom screens are needed as well as slide shows for a dashboard-style overview reports		
	Advanced web	Must have functionality to simulate mouse clicks on a		

	monitoring capabilities	monitored web site and check it for availability and measure response time		
	Templates	It should be possibility to create and deploy monitoring templates on selected servers		
3	**Scoring system calculation**	Deployed Cyber defence exercise scoring system should contain the following futures:	Set	1
		Retrieve continuous monitoring information from Command and control center module		
		Execute team scoring algorithms for every type of cyber defence exercise		
		Be unlocked to modify deployed automated scoring algorithms		
		Be unlocked to develop and deploy new types of automated scoring algorithms for new cyber defence exercises		
		Algorithms source code should be stored, be documented and maintained in the Exercise repository module		
		Display team scores in team displays		
		Display team scores in Command and control center module		
4	**Team performance displays with functionality**	Full HD TV 40 inches with HDMI and USB connectors with the following futures:	Set	4
		Hanged pared on the walls in 2 separate rooms		
		Be configured to display team score and score details in one monitor		
		Be configured to display status of score calculation parameters in the second monitor: is the service (defendable component) running, stopped, etc.		
		Both monitors have to have possibility to be configured to display special messages from Command and control center module, like: additional mission goals, special warnings and other gamification factors relevant to the running scenario		
		Displays configurations should be stored, be documented and maintained in the Exercise repository module		
5	**Version control Capability**	To install, configure and maintain cyber defense exercise source code version control solution with the following futures:	Set	1
	Deployment	Deployment to selected VM located in Server		
	Permissions management	Secure user authentication and availability to limit accessibility to stored components for authenticated users		
	Repository capabilities	Ability to store and control versions of custom, programmable or configurable scenario items: source code, configurations, exploits, injections, attacks scripts, configurations, schedules, scoring parameters, deployment scripts.		
	WikiDocs capability or similar	Ability to prepare, store and control various playbooks for trainees and trainers for whole infrastructure and every cyber defense exercise scenario		

Item-37: Cyber Defence Exercise Module				
SL. #.	**Product Names/Items**	**Description of requirements**	**UoM**	**QTY**
		Cyber Defence Exercise Module provides the exercise scenarios modules		
		Cyber defence exercise module 1: entry level (blue teams competition mode)		
1	**Scenario preparation and deployment**	To prepare cyber defence exercise scenario "entry level (blue teams competition mode)" and deploy it to a mode ready to execute with the following scenario conditions and functionality:	Set	1
	Legend for defendable infrastructure	Each blue team has to defend a network consisting of at least 15 vulnerable assets: VLANs, web applications, FTP, Windows and Linux based legacy systems, DNS, virtual printer, etc. Preconfigured infrastructure should be backed up by using Platform infrastructure and management module Configurable scenario items have to be stored and unlocked for modification in Exercise repository module		
	Legend for attacking	Attacks to the blue teams' vulnerable infrastructure should be executed in an automated and preconfigured way from Training Platform Module in parallel for both teams. Staged attack scenarios should be executed, for example: Stage 1 - attacking websites. Stage 2 - attacking DMZ. Attack types should be at least: • Vulnerability exploitation • SQL injections • DDoS It should be possibility to run advanced attacks manually in addition to the automated attacking baseline if blue teams are performing well. Scripts for automated and manual attacks, exploits, attacks execution baseline, time schedule configurations have to be stored and unlocked for modification in Exercise repository module		
	Legend for scoring system	Scores should be calculated at least for service availability (SLA), proactive defence, and incident reporting and information sharing. Scoring system algorithm and its configurable items have to be stored and unlocked for modification in Exercise repository module		
	Exercise playbook	To provide blue team playbook with objectives, scenarios, goals to achieve, reporting procedures, network and system architecture, and tools. WikiDocs capability or similar from Exercise repository module should be used to document a manual.		
	Exercise management playbook	To provide management playbook material in order to understand architecture, setup and to be able to modify and tune the exercise in the future. WikiDocs capability or similar from Exercise repository module should be used to document a manual.		
		Cyber defence exercise module 2: entry level for a small group		
2	**Scenario preparation and deployment**	To prepare cyber defence exercise scenario "entry level for a small group" and deploy it to a mode ready to execute with the following scenario conditions and functionality:	Set	1
	Legend for	One blue team has to defend a network consisting of at least		

	defendable infrastructure	10 vulnerable assets: web applications, FTP, Windows based legacy system, etc. Preconfigured infrastructure should be backed up by using Platform infrastructure and management module Configurable scenario items have to be stored and unlocked for modification in Exercise repository module		
	Legend for attacking	Attacks to the blue team's vulnerable infrastructure should be executed in an automated and preconfigured way from Training Platform Module. Attack types should be at least: • Anonymous access to a FTP • Vulnerability exploitation • SQL injections • DDoS It should be possibility to run advanced attacks manually in addition to the automated attacking baseline if blue team is performing well. Scripts for automated and manual attacks, exploits, attacks execution baseline, time schedule configurations have to be stored and unlocked for modification in Exercise repository module		
	Legend for scoring system	Scores should be calculated at least for service availability (SLA), proactive defence, and incident reporting and information sharing. Scoring system algorithm and its configurable items have to be stored and unlocked for modification in Exercise repository module		
	Exercise playbook	To provide blue team playbook with objectives, scenarios, goals to achieve, reporting procedures, network and system architecture, and tools. WikiDocs capability or similar from Exercise repository module should be used to document a manual.		
	Exercise management playbook	To provide management playbook material in order to understand architecture, setup and to be able to modify and tune the exercise in the future. WikiDocs capability or similar from Exercise repository module should be used to document a manual.		
		Cyber defence exercise module 3: basic level (blue teams competition mode)		
3	**Scenario preparation and deployment**	To prepare cyber defence exercise scenario "basic level (blue teams competition mode)" and deploy it to a mode ready to execute with the following scenario conditions and functionality:	Set	1
	Legend for defendable infrastructure	Each blue team has to defend and attack an identical network consisting of at least 30 assets: servers, workstations, web and legacy systems, DNS, email, FTP, file servers, domain controller, virtual printer, databases, SCADA servers, etc. Preconfigured infrastructure should be backed up by using Platform infrastructure and management module Configurable scenario items have to be stored and unlocked for modification in Exercise repository module		
	Extended defence functionality	Each team should have possibility to deploy during scenario execution their own (private) virtual machines (VMs) with their own security tools (up to 2)		
	Legend for attacking	Attacks to the blue teams' vulnerable infrastructure should be executed in an automated and preconfigured way from Training Platform Module in parallel for both teams. Staged attack scenarios should be executed, for example: Stage 1 - attacking websites. Stage 2 - attacking DMZ. Stage 3 - attacking applications and private network zones		

		Stage 4 - avalanche (mass destruction with maximum damage attempt) It should be possibility to run advanced attacks manually in addition to the automated attacking baseline if blue teams are performing well. Scripts for automated and manual attacks, exploits, attacks execution baseline, time schedule configurations have to be stored and unlocked for modification in Exercise repository module		
	Legend for scoring system	Scores should be calculated at least for service availability (SLA), proactive defence, and incident reporting and information sharing. Scoring system algorithm and its configurable items have to be stored and unlocked for modification in Exercise repository module		
	Exercise playbook	To provide blue team playbook with objectives, scenarios, goals to achieve, reporting procedures, network and system architecture, and tools. WikiDocs capability or similar from Exercise repository module should be used to document a manual.		
	Exercise management playbook	To provide management playbook material in order to understand architecture, setup and to be able to modify and tune the exercise in the future. WikiDocs capability or similar from Exercise repository module should be used to document a manual.		
		Cyber defence exercise module 4: basic level (capture the flag)		
4	**Scenario preparation and deployment**	To prepare cyber defence exercise scenario “basic level (capture the flag)” and deploy it to a mode ready to execute with the following scenario conditions and functionality:	Set	1
	Legend for blue teams	Each team will play the defender role for their own system and the attacker role for another team's system		
	Legend for exercise infrastructure	Each blue team has to defend and attack an identical network consisting of at least 30 assets: servers, workstations, web and legacy systems, DNS, email, FTP, file sharing, etc. VMs should be different from other exercises. Preconfigured infrastructure should be backed up by using Platform infrastructure and management module Configurable scenario items have to be stored and unlocked for modification in Exercise repository module		
	Extended attacking/defence functionality	Each team should have possibility to deploy during scenario execution their own (private) virtual machines (VMs) with their own defensive and offensive security tools (up to 2)		
	Legend for attacking	Every blue team must try to “capture the flag” located in other’s team infrastructure by using offensive tools.		
	Legend for scoring system	Scores should be calculated at least for service availability (SLA), proactive defence, incident reporting and information sharing. Scoring system algorithm and its configurable items have to be stored and unlocked for modification in Exercise repository module		
	Exercise playbook	To provide blue team playbook with objectives, scenarios, goals to achieve, reporting procedures, network and system architecture, and tools. WikiDocs capability or similar from Exercise repository module should be used to document a manual.		
	Exercise management playbook	To provide management playbook material in order to understand architecture, setup and to be able to modify and tune the exercise in the future. WikiDocs capability or similar from Exercise repository module should be used to document a manual.		

Item-38: Center Operations Manual and Self-Organising Capabilities Module				
SL. #.	**Product Names/Items**	**Description of requirements**	**UoM**	**QTY**
		Center Operations Manual and Self-Organising Capabilities Module ensure quality of the Training operations.		
1	**Operations manual preparation**	Center's operations manual has to be prepared.	Set	1
		It should include technical and organizational setup, highly skilled or advanced work procedures like infrastructure preparation to run an exercise, updating an exercise (versioning, backing up, testing and deploying)		
		WikiDocs capability or similar from Exercise repository module should be used to prepare needed documentation		
2	**Module preparation and deployment**	To prepare self-assessment exercise with zero or entry level cyber security skills with the following scenario conditions and functionality:	Set	1
	Steps based scenario	Trainee is following scenario steps where prepared tasks on Windows/Linux VM should be accomplished. After each task some test questions should be answered and success score automatically calculated		
	Tasks to accomplish	Scenario shall include entry and basic level real live tasks with additional material to read. Tasks include: assessment of effectiveness of incident detection, handling and response, phishing emails where user clicks on infected attachment, vulnerabilities detection, patching activities, system hardening, and configuration management. It should be prepared at least 20 tasks and 20 questions		
	Legend for scoring system	Test-based scoring algorithm and its configurable items have to be stored and unlocked for modification in Exercise repository module		
	Module management playbook	Self-exercise management playbook material should be prepared in order to understand architecture, setup and to be able to modify and tune the exercise in the future. WikiDocs capability or similar from Exercise repository module should be used to prepare needed documentation.		

Item-39: Training Center Operations Functionality Warranty				
SL. #.	**Product Names/Items**	**Description of requirements**	**UoM**	**QTY**
		Training Center Operations Functionality Warranty must be provided to ensure that whole training center is delivering expect Functionality. It incorporates Skills deployment activities for centre's manager and trainers, as well as Operating the Exercises.		
1	**Skills deployment activities**	Selected center manager and trainers should be prepared to run the center by conducting the following activities:	Set	1
		Detail explanation on every project item onsite for at least 5 working days		
		Switching team accounts into privileged		
		Unit running sessions by following Center operations manual for the whole delivery period for item Running exercises, including 5 working days before and after execution		
2	**Exercise Pilot**	Every exercise shall be executed with Consultant's presence	Set	8

	Execution	for external constituency at least for 2 times.		
	Quality improvement	Feedback for the exercise setup, execution and results should be collected after every event, then summarized, discussed with the Purchaser and infrastructure and exercise setup improvement actions should be conducted when necessary		
3	**Exercise Provisioning**	Every exercise shall be executed with Consultant's presence for external constituency, per week there should be at least two exercises provisioned when requested and executed, where supplier staff must provide at least one person full time for whole week period to instruct, prepare, run and lead the training. Additional assistants (up to 3) are possible to inquire via Client from Academia	Week	72

Item-40: Automation and Orchestration				
SL. #.	**Product Names/Items**	**Description of requirements**	**UoM**	**QTY**
1	Test Automation and Infrastructure Orchestration,	Qualisystems Cloud Shell Annual Subscription SMALL Active Environment Bundle (SKU QS-QSB-S). Must include three (3) years of warranty, maintenance, and support from OEM; Must Provide five (5) Active Environments (5 x QS-ENV) and the following: ➢ 1 Authoring License (1 x QS-AUTH) ➢ 1 Application Server License (1 x QS-AS) ➢ 1 Authoring License ➢ 1 Application Server License	Set	1

E. TESTING AND QUALITY ASSURANCE REQUIREMENTS

4.1 Inspections

4.1.1 Factory Inspections: No factory inspection from the Purchaser is necessary.

3.1.2 Inspections following delivery shall be arranged in the office of the Project Director or in a designated location as per the instruction of the office of the project director. The inspection activities will include checks whether the hardware and software supplied under this tender comply with the minimum requirements set forth in the technical requirements section of this tender. It will also check the physical condition of the items as well as ingenuity of their source and other obligations mentioned in this tender document and the agreement signed between the purchaser and the selected vendor.

4.2 Pre-commissioning Tests

4.2.0 In addition to the Supplier's standard check-out and set-up tests, the Supplier (with the assistance of the Purchaser) must perform the following tests on the System and its Subsystems before Installation will be deemed to have occurred and the Purchaser will issue the Installation Certificate(s) (pursuant to GCC Clause 26 and related SCC clauses).

4.2.1 Test of all individual software systems must be performed and desired performance indicators and technical specifications mentioned in this tender must be met by each and every software component / system included in this tender.

4.2.2 Test of all individual hardware components must be performed and desired performance indicators and technical specifications mentioned in this tender must be met by each and every hardware component / system included in this tender.

4.2. 3 The Entire System: Pre-commissioning Tests for the entire System must be performed and the entire platform of Cyber Sensors must operate as an integrated system and fulfill all performance requirements of the information system stated above in point # 1.5 of section B (Functional, Architectural and Performance Requirements).

4.3 Operational Acceptance Tests

4.3.0 Pursuant to GCC Clause 27 and related SCC clauses, the Purchaser (with the assistance of the Supplier) will perform the following tests on the System and its Subsystems following Installation to determine whether the System and the Subsystems meet all the requirements mandated for Operational Acceptance.

4.3.1 The Purchaser (with the assistance of the Supplier) shall perform Operational Acceptance Tests to ascertain whether the System, or a specified Subsystem, is able to attain the functional and performance requirements specified in the Technical

Requirements and Agreed and Finalized Project Plan, in accordance with the provisions of GCC Clause 27.2 (Operational Acceptance Test).

The Supplier shall use all reasonable endeavors to promptly remedy any defect and/or deficiencies and/or other reasons for the failure of the Operational Acceptance Test that the Project Manager has notified the Supplier of. Once such remedies have been made by the Supplier, the Supplier shall notify the Purchaser, and the Purchaser, with the full cooperation of the Supplier, shall use all reasonable endeavors to promptly carry out retesting of the System or Subsystem. Upon the successful conclusion of the Operational Acceptance Tests, the Supplier shall notify the Purchaser of its request for Operational Acceptance Certification, in accordance with GCC Clause 27.3.3. The Purchaser shall then issue to the Supplier the Operational Acceptance Certification in accordance with GCC Clause 27.3.3 (a), or shall notify the Supplier of further defects, deficiencies, or other reasons for the failure of the Operational Acceptance Test. The procedure set out in this GCC Clause 27.3.4 shall be repeated, as necessary, until an Operational Acceptance Certificate is issued.

The Supplier shall submit the system integration test report detailing the test results from the successful completion of the tests to the purchaser for review at least two (2) weeks before the commencement of the OAT. The Government reserves the right to hold back the OAT until the evidence of the successful completion of the tests is produced.

F. SERVICE SPECIFICATIONS – RECURRENT COST ITEMS

5.1 Warranty Defect Repair

5.1.1 The Supplier MUST provide the following services under the Contract or, as appropriate under separate contracts (as specified in the bidding documents).

5.1.1.1 Warranty Defect Repair Service: Three (3) years warranty should provide to all equipments, systems, and hardware and software items; furthermore three (3) years software licenses of each and every system/solution must be factored along with three years full support including labor, spare parts, updates and/or upgrades.

5.1.1.2 Technical Assistance: Supplier should provide Technical assistance on call basis during warranty period. Response time must be less than 2 hours and resolution time must be less than 6 hours.

Important Note: *All costs of the above mentioned services must be included as one time cost in the bidding price. There will be no recurrent cost items in this tender.*

5.2 Technical Support

5.2.1 The Supplier MUST provide the following services under the Contract or, as appropriate under separate contracts (as specified in the bidding documents).

5.2.1.1 User support / hot line: Not Applicable

5.2.1.2 Technical Assistance: Not Applicable

5.2.1.3 Post-Warranty Maintenance Services: Not Applicable

5.3 Requirements of the Supplier's Technical Team

5.3.1 The Supplier MUST provide a technical team to cover the Purchaser's anticipated Post-Operational Acceptance Technical Assistance Activities Requirements (e.g., modification of the Information System to comply with changing legislation and regulations) with the roles and skill levels that are specified below. The minimum expected quantities of inputs by the Supplier's technical support team are specified in the relevant System Inventory Tables for Recurrent Cost Items.

5.3.1.1 Requirements mentioned above in point 2.7 (Requirements of the Supplier's Technical Team) is also applicable for Post-Operational Acceptance Technical Assistance Activities.

Implementation Schedule

Notes on preparing the Implementation Schedule

The Implementation Schedule summarize when and where Installation, and Operational Acceptance should take place for all Subsystems and/or major components of the System, and for the overall System itself – as well as any other major Contract milestones.

Note: The delivery date is not presented in the Implementation Schedule. Under Incoterms 2010 for CIP, Delivery refers to the date when the Supplier delivers the goods to the first carrier at the port of embarkation, not to the arrival of the goods at the destination site. Delivery (shipment) date therefore varies according to the country of origin of the goods and the Supplier's chosen method of transport.

The target dates need to be realistic and achievable in light of the capacity of both the average Supplier and the Purchaser to carry out their respective contract obligations. Also, the Purchaser must take care to ensure that the dates specified in the Schedule are consistent with any specified elsewhere in the bidding document, especially in the GCC/SCC (e.g., and/or times specified for the submission and acceptance of the Agreed Project Plan).

The work breakdown structure (deliverables) in the Implementation Schedule should be sufficiently detailed to facilitate careful management of the Contract – but not so detailed that it unnecessarily constrains bidders from organizing the proposed work in the most efficient and effective manner.

To facilitate the bidding and the contract management processes, the Implementation Schedule, the System Inventory Tables and Price Schedules should be closely linked. In particular, the Implementation Schedule defines the major deliverable Subsystems. For each Subsystem there should be a corresponding System Inventory Table or Tables. These System Inventory Tables catalog the specific items (inputs) comprising the Subsystem, as well as the quantities of each item required (for the supply and install cost items as well as the recurrent cost items). For each System Inventory Table there should be a corresponding Price Schedule that closely mirrors the System Inventory Table. Careful development of these materials will greatly improve the changes of obtaining complete and comparable bids (and ease the bid evaluation process) as well as improving the likelihood that the Purchaser's and Supplier's interactions during contract execution are closely orchestrated (thus easing the burden of contract management and improving the likelihood of successful implementation of the Information System).

The sample tables comprise:

(a) An Implementation Schedule Table;

(b) A Site Table(s); and

(c) A Table of Holidays and other Non-Working Days.

The Purchaser should modify these tables, as required, to suit the particulars of the System (and Subsystems) to be supplied and installed. The sample text in the tables is illustrative only and should be modified or deleted as appropriate.

The timings stated in the Implementation Schedule should be specified in weeks from Contract Effectiveness. This will ease the maintenance of the bidding documents during the preparation and bidding processes.

Where appropriate, the Implementation Schedule should indicate the deliverables against which Liquidated Damages may be applied in the event of implementation delays arising from the actions of the Supplier (as governed by the SCC and GCC clause 28). These milestones should be kept to the essential minimum needed by the Purchaser to ensure contract discipline by the Supplier – but not so many that they unnecessarily strain the Purchaser-Supplier relationship upon which the successful implementation of the Information System will invariably depend.

The Site Table(s) catalog the physical location of the site(s) where the System is to be supplied, installed, and operated. The site(s) may consist of a number of branch offices in remote regions, different departments or offices in the same city, or a combination of these. The Purchaser must specify this information in sufficient detail so that Bidders can accurately estimate costs related to:

(a) Delivery and insurance;

(b) Installation, including cabling and inter-building communications, etc.

(c) Perform support services, such as warranty defect repair, maintenance, and other technical support services; and

(d) Other related Service obligations the successful Bidder will have to perform under the Contract, including related travel and subsistence costs.

This information will also help Bidders identify which site(s) may warrant a site visit during the period they are preparing their bids. If the System presents complex installation challenges, site layout drawings should be included in the Background and Informational Materials Section.

Table of Contents: Implementation Schedule

A. IMPLEMENTATION SCHEDULE TABLE

*[Specify **desired installation and acceptance dates for all items in Schedule below, modifying the sample line items and sample table entries as needed.]***

Line Item No.	Subsystem / Item	Configuration Table No.	Site / Site Code	Delivery (Bidder to specify in the Preliminary Project Plan)	Installation (weeks from Effective Date)	Acceptance (weeks from Effective Date)	Liquidated Damages Milestone
1	Detailed design of the implementation of the Cyber Attack Simulation						
2	Applications and Security Testing Appliance						
3	Application and Threat Intelligence Program						
4	Application Server						
5	Interfaces						
6	Analog Platform						
7	Server						
8	Workstation						
9	Whiteboard						
10	Monitor						
11	PoE Switch (24 Port)						

Line Item No.	Subsystem / Item	Configuration Table No.	Site / Site Code	Delivery (Bidder to specify in the Preliminary Project Plan)	Installation (weeks from Effective Date)	Acceptance (weeks from Effective Date)	Liquidated Damages Milestone
12	PoE Switch (48 Port)						
13	Router (Type-1)						
14	Router (Type-2)						
15	Network Management System (NMS)						
16	Wireless Location & Wireless Intrusion Prevention System						
17	Virtual Switching Software						
18	Mail Security System						
19	Web Security System						
20	Virtual Firewall						
21	Virtual Instruction Prevention System						
22	End-Point Malware Protection Software						
23	Security Management System						
24	Network Behavior Analysis System						
25	Network Access Control and Authentication System						

Line Item No.	Subsystem / Item	Configuration Table No.	Site / Site Code	Delivery (Bidder to specify in the Preliminary Project Plan)	Installation (weeks from Effective Date)	Acceptance (weeks from Effective Date)	Liquidated Damages Milestone
26	Wireless Access Point						
27	Hyper-Visor, VDI & Hyper-Visor Management System						
28	SAN Switch						
29	Storage Server						
30	Firewall (Type-1)						
31	Firewall (Type-2)						
32	SIEM and Data Analytics System						
33	Industrial Switch (Type-1)						
34	Industrial Switch (Type-2)						
35	Industrial Router						
36	Training Platform Module						
37	Cyber Defence Exercise Module						
38	Center Operations Manual and Self-Organising Capabilities Module						
39	Training Center Operations Functionality Warranty						

Line Item No.	Subsystem / Item	Configuration Table No.	Site / Site Code	Delivery (Bidder to specify in the Preliminary Project Plan)	Installation (weeks from Effective Date)	Acceptance (weeks from Effective Date)	Liquidated Damages Milestone
40	Automation and Orchestration						

Note: Refer to the System Inventory Table(s) for the specific items and components that constitute the Subsystems or item. Refer to the Site Table(s) below for details regarding the site and the site code.

- - indicates not applicable. "Indicates repetition of table entry above.

B. SITE TABLE(S)

[Specify: ***the detailed information regarding the site(s) at which the System is to be operated****]*

Site Code	Site	City / Town / Region	Primary Street Address	Drawing Reference No. (if any)

C. TABLE OF HOLIDAYS AND OTHER NON-WORKING DAYS

[Specify: ***the days for each month for each year that are non-working days, due to Holidays or other business reasons (other than weekends).****]*

Month	20xy	20xy+1	20xy+2	....			...	20zz
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								
11								
12								

System Inventory Tables

Notes on preparing the System Inventory Tables

The System Inventory Tables detail:

(a) For each Subsystem (Deliverable) indicated in the Implementation Schedule, the Information Technologies, Materials, and other Goods and Services that comprise the System to be supplied and/or performed by the Supplier;

(b) The quantities of such Information Technologies, Materials, and other Goods and Services;

(c) The sites and the location of each on a specific site (e.g., building, floor, room, department, etc.)

(d) The cross references to the relevant section of the Technical Requirements where that item is described in greater detail

The Purchaser should modify these tables, as required, to suit the particulars of the System (and Subsystems) to be supplied and installed. The sample text provided for various sections of the tables is illustrative only and should be modified or deleted as appropriate.

There are two sample formats given for the System Inventory Tables: one for the Supply and Installation cost items and the second for recurrent cost items needed (if any). The second version of the table permits the Purchaser to obtain price information about items that are needed during the Warranty Period.

Table of Contents: System Inventory Tables

SYSTEM INVENTORY TABLE (SUPPLY AND INSTALLATION COST ITEMS) *[INSERT: IDENTIFYING NUMBER]*

Line item number: *[specify:* ***relevant line item number from the Implementation Schedule (e.g., 1.1)*** *]*

[as necessary for the supply and installation of the System, specify: ***the detailed components and quantities in the System Inventory Table below for the line item specified above, modifying the sample components and sample table entries as needed.*** *Repeat the System Inventory Table as needed to cover each and every line item in the Implementation Schedule that requires elaboration.]*

Component No.	Component	Relevant Technical Specifications No.	Additional Site Information (e.g., building, floor, department, etc.)	Quantity
1.	Subsystem 1		- -	- -
1.1	_____			- -
:				
2.	Subsystem 2			- -
2.1	_____			- -
:				

Note: - - indicates not applicable. " indicates repetition of table entry above.

SYSTEM INVENTORY TABLE (RECURRENT COST ITEMS) ***[INSERT: IDENTIFYING NUMBER] –***

Line item number: *[specify:* ***relevant line item number from the Implementation Schedule (e.g., y.1)*** *]*

Component No.	Component	Relevant Technical Specifications No.	Y1	Y2	Y3
1.	Warranty/ Defect Repair/Replacement		all items, all sites, included in the Supply and Install Price	all items, all sites, included in the Supply and Install Price	all items, all sites, included in the Supply and Install Price
2.	Software/Firmware Licenses and Updates:		all items, all sites, included in the Supply and Install Price	all items, all sites, included in the Supply and Install Price	all items, all sites, included in the Supply and Install Price
3.	Technical Services		all items, all sites, included in the Supply and Install Price	all items, all sites, included in the Supply and Install Price	all items, all sites, included in the Supply and Install Price
3.1					
3.2					
3.3					
	…				

Note: - - indicates not applicable. "Indicates repetition of table entry above.

Background and Informational Materials

Notes on Background and Informational Materials

This section of the bidding document provides a place to gather materials that the Purchaser believes will help Bidders prepare more precisely targeted technical bids and more precise bid prices.

These materials MUST NOT introduce requirements for the Information System. Rather they should assist Bidders to interpret the Technical Requirements and the General and Specific Conditions of Contract. For example, these Background and Informational Materials may describe existing information systems that the Information System to be supplied and installed under the Contract must integrate with. However, the specific requirement that the Supplier must integrate the Information System with other systems needs to be stated in the Technical Requirements. Similarly, these Background and Informational Materials may describe the legal and regulatory norms (including for example statutory report formats) that are relevant to the Information System. The Technical Requirements Section would need to spell out that the Supplier must ensure the Information System complies with the relevant legal and regulatory norms.

Table of Contents: Background and Informational Materials

Background and Informational Materials

Note: The following is only a sample outline. Entries should be modified, extended, and/or deleted, as appropriate for the particular System to be supplied and installed. DO NOT introduce requirements for the System in this section.

A. BACKGROUND

0.1 The Purchaser

0.1.1 *[provide: an overview of the Agency's legal basis, organizational role, and core objectives]*

0.1.2 *[provide: an overview of the stakeholders to the Information System*

0.1.3 *[provide: an overview of the Purchaser's project management and decision-making arrangements applicable to the System and performance of the Contract]*

0.2 The Purchaser's Business Objectives for the Information System

0.2.1 *[provide: an overview of the current business objectives, procedures, and processes and how they will be affected by the System]*

0.2.2 *[provide: an overview of the changes in objectives, procedures, and processes to be made possible by the System]*

0.2.3 *[provide: a brief description of the expected benefits of the System]*

B. INFORMATIONAL MATERIALS

0.3 The Legal, Regulatory, and Normative Context for the Information System

0.3.1 *[provide: an overview of the laws, regulations and other formal norm which will shape the Information System.]*

0.3.2 *[provide: samples of existing standardized reports, data entry forms, data formats, data coding schemes, etc. which the Information System will need to implement.]*

0.4 Existing Information Systems / Information Technologies Relevant to the Information System

0.4.1 *[provide: an overview of the existing information systems and information technologies which will establish the technological context for the implementation of the Information System.]*

0.4.2 *[provide: an overview of the ongoing or planned information systems initiatives that will shape context for the implementation of the Information System.]*

0.5 Available Training Facilities to Support the Implementation of the Information System

0.5.1 *[provide: an overview of the Purchaser's existing training facilities that would be available to support the implementation of the Information System.]*

0.6 Site Drawings and Site Survey Information Relevant to the Information System

0.6.1 *[provide: information of the sites at which the Information System would be implemented.]*

PART 3 – CONDITIONS OF CONTRACT AND CONTRACT FORMS

SECTION VIII - GENERAL CONDITIONS OF CONTRACT

Table of Clauses

General Conditions of Contract

A. CONTRACT AND INTERPRETATION

1. Definitions

1.1 In this Contract, the following terms shall be interpreted as indicated below.

(a) contract elements

(i) "Contract" means the Contract Agreement entered into between the Purchaser and the Supplier, together with the Contract Documents referred to therein. The Contract Agreement and the Contract Documents shall constitute the Contract, and the term "the Contract" shall in all such documents be construed accordingly.

(ii) "Contract Documents" means the documents specified in Article 1.1 (Contract Documents) of the Contract Agreement (including any amendments to these Documents).

(iii) "Contract Agreement" means the agreement entered into between the Purchaser and the Supplier using the form of Contract Agreement contained in the Sample Contractual Forms Section of the bidding documents and any modifications to this form agreed to by the Purchaser and the Supplier. The date of the Contract Agreement shall be recorded in the signed form.

(iv) "GCC" means the General Conditions of Contract.

(v) "SCC" means the Special Conditions of Contract.

(vi) "Technical Requirements" means the Technical Requirements in Section VII of the bidding documents.

(vii) "Implementation Schedule" means the Implementation Schedule in Section VII of the bidding documents.

viii) "Contract Price" means the price or prices defined in Article 2 (Contract Price and Terms of Payment) of the Contract Agreement.

(ix) "Procurement Regulations" refers to the edition **specified in the SCC** of the World Bank "Procurement Regulations for IPF Borrowers".

(x) "bidding documents" refers to the collection of documents issued by the Purchaser to instruct and inform potential suppliers of the processes for bidding, selection of the winning bid, and Contract formation, as well as the contractual conditions governing the relationship between the Purchaser and the Supplier. The General and Special Conditions of Contract, the Technical Requirements, and all other documents included in the bidding documents reflect the Procurement Regulations that the Purchaser is obligated to follow during procurement and administration of this Contract.

(b) entities

(i) "Purchaser" means the entity purchasing the Information System, as **specified in the SCC.**

(ii) "Project Manager" means the person **named as such in the SCC** or otherwise appointed by the Purchaser in the manner provided in GCC Clause 18.1 (Project Manager) to perform the duties delegated by the Purchaser.

(iii) "Supplier" means the firm or Joint Venture whose bid to perform the Contract has been accepted by the Purchaser and is named as such in the Contract Agreement.

(iv) "Supplier's Representative" means any person nominated by the Supplier and named as such in the Contract Agreement or otherwise approved by the Purchaser in the manner provided in GCC Clause 18.2 (Supplier's Representative) to perform the duties delegated by the Supplier.

(v) "Subcontractor" means any firm to whom any of the obligations of the Supplier, including preparation of any design or supply of any

Information Technologies or other Goods or Services, is subcontracted directly or indirectly by the Supplier.

(vi) "Adjudicator" means the person named in Appendix 2 of the Contract Agreement, appointed by agreement between the Purchaser and the Supplier to make a decision on or to settle any dispute between the Purchaser and the Supplier referred to him or her by the parties, pursuant to GCC Clause 6.1 (Adjudication).

(vii) "The World Bank" (also called "The Bank") means the International Bank for Reconstruction and Development (IBRD) or the International Development Association (IDA).

(c) scope

(i) "Information System," also called "the System," means all the Information Technologies, Materials, and other Goods to be supplied, installed, integrated, and made operational (exclusive of the Supplier's Equipment), together with the Services to be carried out by the Supplier under the Contract.

(ii) "Subsystem" means any subset of the System identified as such in the Contract that may be supplied, installed, tested, and commissioned individually before Commissioning of the entire System.

(iii) "Information Technologies" means all information processing and communications-related hardware, Software, supplies, and consumable items that the Supplier is required to supply and install under the Contract.

(iv) "Goods" means all equipment, machinery, furnishings, Materials, and other tangible items that the Supplier is required to supply or supply and install under the Contract, including, without limitation, the Information Technologies and Materials, but excluding the Supplier's Equipment.

(v) "Services" means all technical, logistical,

management, and any other Services to be provided by the Supplier under the Contract to supply, install, customize, integrate, and make operational the System. Such Services may include, but are not restricted to, activity management and quality assurance, design, development, customization, documentation, transportation, insurance, inspection, expediting, site preparation, installation, integration, training, data migration, Pre-commissioning, Commissioning, maintenance, and technical support.

(vi) "The Project Plan" means the document to be developed by the Supplier and approved by the Purchaser, pursuant to GCC Clause 19, based on the requirements of the Contract and the Preliminary Project Plan included in the Supplier's bid. The "Agreed Project Plan" is the version of the Project Plan approved by the Purchaser, in accordance with GCC Clause 19.2. Should the Project Plan conflict with the Contract in any way, the relevant provisions of the Contract, including any amendments, shall prevail.

(vii) "Software" means that part of the System which are instructions that cause information processing Subsystems to perform in a specific manner or execute specific operations.

(viii) "System Software" means Software that provides the operating and management instructions for the underlying hardware and other components, and is identified as such in Appendix 4 of the Contract Agreement and such other Software as the parties may agree in writing to be Systems Software. Such System Software includes, but is not restricted to, micro-code embedded in hardware (i.e., "firmware"), operating systems, communications, system and network management, and utility software.

(ix) "General-Purpose Software" means Software that supports general-purpose office and software development activities and is identified as such in Appendix 4 of the Contract

Agreement and such other Software as the parties may agree in writing to be General-Purpose Software. Such General-Purpose Software may include, but is not restricted to, word processing, spreadsheet, generic database management, and application development software.

(x) "Application Software" means Software formulated to perform specific business or technical functions and interface with the business or technical users of the System and is identified as such in Appendix 4 of the Contract Agreement and such other Software as the parties may agree in writing to be Application Software.

(xi) "Standard Software" means Software identified as such in Appendix 4 of the Contract Agreement and such other Software as the parties may agree in writing to be Standard Software.

(xii) "Custom Software" means Software identified as such in Appendix 4 of the Contract Agreement and such other Software as the parties may agree in writing to be Custom Software.

(xiii) "Source Code" means the database structures, dictionaries, definitions, program source files, and any other symbolic representations necessary for the compilation, execution, and subsequent maintenance of the Software (typically, but not exclusively, required for Custom Software).

(xiv) "Materials" means all documentation in printed or printable form and all instructional and informational aides in any form (including audio, video, and text) and on any medium, provided to the Purchaser under the Contract.

(xv) "Standard Materials" means all Materials not specified as Custom Materials.

(xvi) "Custom Materials" means Materials developed by the Supplier at the Purchaser's expense under the Contract and identified as such in Appendix 5

of the Contract Agreement and such other Materials as the parties may agree in writing to be Custom Materials. Custom Materials includes Materials created from Standard Materials.

(xvii) "Intellectual Property Rights" means any and all copyright, moral rights, trademark, patent, and other intellectual and proprietary rights, title and interests worldwide, whether vested, contingent, or future, including without limitation all economic rights and all exclusive rights to reproduce, fix, adapt, modify, translate, create derivative works from, extract or re-utilize data from, manufacture, introduce into circulation, publish, distribute, sell, license, sublicense, transfer, rent, lease, transmit or provide access electronically, broadcast, display, enter into computer memory, or otherwise use any portion or copy, in whole or in part, in any form, directly or indirectly, or to authorize or assign others to do so.

(xviii) "Supplier's Equipment" means all equipment, tools, apparatus, or things of every kind required in or for installation, completion and maintenance of the System that are to be provided by the Supplier, but excluding the Information Technologies, or other items forming part of the System.

(d) activities

(i) "Delivery" means the transfer of the Goods from the Supplier to the Purchaser in accordance with the current edition Incoterms specified in the Contract.

(ii) "Installation" means that the System or a Subsystem as specified in the Contract is ready for Commissioning as provided in GCC Clause 26 (Installation).

(iii) "Pre-commissioning" means the testing, checking, and any other required activity that may be specified in the Technical Requirements that are to be carried out by the Supplier in preparation for Commissioning of the System as provided in GCC

Clause 26 (Installation).

(iv) "Commissioning" means operation of the System or any Subsystem by the Supplier following Installation, which operation is to be carried out by the Supplier as provided in GCC Clause 27.1 (Commissioning), for the purpose of carrying out Operational Acceptance Test(s).

(v) "Operational Acceptance Tests" means the tests specified in the Technical Requirements and Agreed Project Plan to be carried out to ascertain whether the System, or a specified Subsystem, is able to attain the functional and performance requirements specified in the Technical Requirements and Agreed Project Plan, in accordance with the provisions of GCC Clause 27.2 (Operational Acceptance Test).

(vi) "Operational Acceptance" means the acceptance by the Purchaser of the System (or any Subsystem(s) where the Contract provides for acceptance of the System in parts), in accordance with GCC Clause 27.3 (Operational Acceptance).

(e) place and time

(i) "Purchaser's Country" is the **country named in the SCC.**

(ii) "Supplier's Country" is the country in which the Supplier is legally organized, as named in the Contract Agreement.

(iii) **Unless otherwise specified in the SCC** "Project Site(s)" means the place(s) in the Site Table in the Technical Requirements Section for the supply and installation of the System.

(iv) "Eligible Country" means the countries and territories eligible for participation in procurements financed by the World Bank as defined in the Procurement Regulations.

(v) "Day" means calendar day of the Gregorian Calendar.

(vi) "Week" means seven (7) consecutive Days,

beginning the day of the week as is customary in the Purchaser's Country.

(vii) "Month" means calendar month of the Gregorian Calendar.

(viii) "Year" means twelve (12) consecutive Months.

(ix) "Effective Date" means the date of fulfillment of all conditions specified in Article 3 (Effective Date for Determining Time for Achieving Operational Acceptance) of the Contract Agreement, for the purpose of determining the Delivery, Installation, and Operational Acceptance dates for the System or Subsystem(s).

(x) "Contract Period" is the time period during which this Contract governs the relations and obligations of the Purchaser and Supplier in relation to the System, as **unless otherwise specified in the SCC,** the Contract shall continue in force until the Information System and all the Services have been provided, unless the Contract is terminated earlier in accordance with the terms set out in the Contract**.**

(xi) "Defect Liability Period" (also referred to as the "Warranty Period") means the period of validity of the warranties given by the Supplier commencing at date of the Operational Acceptance Certificate of the System or Subsystem(s), during which the Supplier is responsible for defects with respect to the System (or the relevant Subsystem[s]) as provided in GCC Clause 29 (Defect Liability).

(xii) "The Coverage Period" means the Days of the Week and the hours of those Days during which maintenance, operational, and/or technical support services (if any) must be available.

(xiii) The Post-Warranty Services Period" means the number of years **defined in the SCC** (if any), following the expiration of the Warranty Period during which the Supplier may be obligated to provide Software licenses, maintenance, and/or technical support services for the System, either

under this Contract or under separate contract(s).

2. Contract Documents

2.1 Subject to Article 1.2 (Order of Precedence) of the Contract Agreement, all documents forming part of the Contract (and all parts of these documents) are intended to be correlative, complementary, and mutually explanatory. The Contract shall be read as a whole.

3. Interpretation

3.1 Governing Language

3.1.1 **Unless otherwise specified in the SCC**, all Contract Documents and related correspondence exchanged between Purchaser and Supplier shall be written in the language of these bidding documents (English)**,** and the Contract shall be construed and interpreted in accordance with that language.

3.1.2 If any of the Contract Documents or related correspondence are prepared in a language other than the governing language under GCC Clause 3.1.1 above, the translation of such documents into the governing language shall prevail in matters of interpretation. The originating party, with respect to such documents shall bear the costs and risks of such translation.

3.2 Singular and Plural

The singular shall include the plural and the plural the singular, except where the context otherwise requires.

3.3 Headings

The headings and marginal notes in the GCC are included for ease of reference and shall neither constitute a part of the Contract nor affect its interpretation.

3.4 Persons

Words importing persons or parties shall include firms, corporations, and government entities.

3.5 Incoterms

Unless inconsistent with any provision of the Contract, the meaning of any trade term and the rights and obligations of parties thereunder shall be as prescribed by the Incoterms

Incoterms means international rules for interpreting trade terms published by the International Chamber of Commerce

(latest edition), 38 Cours Albert 1er, 75008 Paris, France.

3.6 Entire Agreement

The Contract constitutes the entire agreement between the Purchaser and Supplier with respect to the subject matter of Contract and supersedes all communications, negotiations, and agreements (whether written or oral) of parties with respect to the subject matter of the Contract made prior to the date of Contract.

3.7 Amendment

No amendment or other variation of the Contract shall be effective unless it is in writing, is dated, expressly refers to the Contract, and is signed by a duly authorized representative of each party to the Contract.

3.8 Independent Supplier

The Supplier shall be an independent contractor performing the Contract. The Contract does not create any agency, partnership, joint venture, or other joint relationship between the parties to the Contract.

Subject to the provisions of the Contract, the Supplier shall be solely responsible for the manner in which the Contract is performed. All employees, representatives, or Subcontractors engaged by the Supplier in connection with the performance of the Contract shall be under the complete control of the Supplier and shall not be deemed to be employees of the Purchaser, and nothing contained in the Contract or in any subcontract awarded by the Supplier shall be construed to create any contractual relationship between any such employees, representatives, or Subcontractors and the Purchaser.

3.9 Joint Venture

If the Supplier is a Joint Venture of two or more firms, all such firms shall be jointly and severally bound to the Purchaser for the fulfillment of the provisions of the Contract and shall designate one of such firms to act as a leader with authority to bind the Joint Venture. The composition or constitution of the Joint Venture shall not be altered without the prior consent of the Purchaser.

3.10 Nonwaiver

3.10.1 Subject to GCC Clause 3.10.2 below, no relaxation, forbearance, delay, or indulgence by either party in enforcing any of the terms and conditions of the Contract or the granting of time by either party to the other shall prejudice, affect, or restrict the rights of that party under the Contract, nor shall any waiver by either party of any breach of Contract operate as waiver of any subsequent or continuing breach of Contract.

3.10.2 Any waiver of a party's rights, powers, or remedies under the Contract must be in writing, must be dated and signed by an authorized representative of the party granting such waiver, and must specify the right and the extent to which it is being waived.

3.11 Severability

If any provision or condition of the Contract is prohibited or rendered invalid or unenforceable, such prohibition, invalidity, or unenforceability shall not affect the validity or enforceability of any other provisions and conditions of the Contract.

3.12 Country of Origin

"Origin" means the place where the Information Technologies, Materials, and other Goods for the System were produced or from which the Services are supplied. Goods are produced when, through manufacturing, processing, Software development, or substantial and major assembly or integration of components, a commercially recognized product results that is substantially different in basic characteristics or in purpose or utility from its components. The Origin of Goods and Services is distinct from the nationality of the Supplier and may be different.

4. Notices

4.1 Unless otherwise stated in the Contract, all notices to be given under the Contract shall be in writing and shall be sent, pursuant to GCC Clause 4.3 below, by personal delivery, airmail post, special courier, facsimile, electronic mail, or Electronic Data Interchange (EDI), with the following provisions.

4.1.1 Any notice sent by facsimile, electronic mail, or EDI shall be confirmed within two (2) days after dispatch

by notice sent by airmail post or special courier, except as otherwise specified in the Contract.

4.1.2 Any notice sent by airmail post or special courier shall be deemed (in the absence of evidence of earlier receipt) to have been delivered ten (10) days after dispatch. In proving the fact of dispatch, it shall be sufficient to show that the envelope containing such notice was properly addressed, stamped, and conveyed to the postal authorities or courier service for transmission by airmail or special courier.

4.1.3 Any notice delivered personally or sent by facsimile, electronic mail, or EDI shall be deemed to have been delivered on the date of its dispatch.

4.1.4 Either party may change its postal, facsimile, electronic mail, or EDI addresses for receipt of such notices by ten (10) days' notice to the other party in writing.

4.2 Notices shall be deemed to include any approvals, consents, instructions, orders, certificates, information and other communication to be given under the Contract.

4.3 Pursuant to GCC Clause 18, notices from/to the Purchaser are normally given by, or addressed to, the Project Manager, while notices from/to the Supplier are normally given by, or addressed to, the Supplier's Representative, or in its absence its deputy if any. If there is no appointed Project Manager or Supplier's Representative (or deputy), or if their related authority is limited by the SCC for GCC Clauses 18.1 or 18.2.2, or for any other reason, the Purchaser or Supplier may give and receive notices at their fallback addresses. The address of the Project Manager and the fallback address of the Purchaser are as **specified in the SCC** or as subsequently established/amended. The address of the Supplier's Representative and the fallback address of the Supplier are as specified in Appendix 1 of the Contract Agreement or as subsequently established/amended.

5. Governing Law

5.1 The Contract shall be governed by and interpreted in accordance with the laws of the country **specified in the SCC**.

5.2 Throughout the execution of the Contract, the Supplier shall comply with the import of goods and services prohibitions in the Purchaser's Country when

(a) as a matter of law or official regulations, the Borrower's country prohibits commercial relations with that country; or

5.3 by an act of compliance with a decision of the United Nations Security Council taken under Chapter VII of the Charter of the United Nations, the Borrower's Country prohibits any import of goods from that country or any payments to any country, person, or entity in that country.

6. Fraud and Corruption

6.1 The Bank requires compliance with the Bank's Anti-Corruption Guidelines and its prevailing sanctions policies and procedures as set forth in the WBG's Sanctions Framework, as set forth in the Appendix to the GCC.

6.2 The Purchaser requires the Supplier to disclose any commissions or fees that may have been paid or are to be paid to agents or any other party with respect to the bidding process or execution of the Contract. The information disclosed must include at least the name and address of the agent or other party, the amount and currency, and the purpose of the commission, gratuity or fee.

B. SUBJECT MATTER OF CONTRACT

7. Scope of the System

7.1 Unless otherwise expressly **limited in the SCC** or Technical Requirements, the Supplier's obligations cover the provision of all Information Technologies, Materials and other Goods as well as the performance of all Services required for the design, development, and implementation (including procurement, quality assurance, assembly, associated site preparation, Delivery, Pre-commissioning, Installation, Testing, and Commissioning) of the System, in accordance with the plans, procedures, specifications, drawings, codes, and any other documents specified in the Contract and the

Agreed Project Plan.

7.2 The Supplier shall, unless specifically excluded in the Contract, perform all such work and / or supply all such items and Materials not specifically mentioned in the Contract but that can be reasonably inferred from the Contract as being required for attaining Operational Acceptance of the System as if such work and / or items and Materials were expressly mentioned in the Contract.

7.3 The Supplier's obligations (if any) to provide Goods and Services as implied by the Recurrent Cost tables of the Supplier's bid, such as consumables, spare parts, and technical services (e.g., maintenance, technical assistance, and operational support), are as **specified in the SCC,** including the relevant terms, characteristics, and timings.

8. Time for Commencement and Operational Acceptance

8.1 The Supplier shall commence work on the System within the period **specified in the SCC,** and without prejudice to GCC Clause 28.2, the Supplier shall thereafter proceed with the System in accordance with the time schedule specified in the Implementation Schedule and any refinements made in the Agreed Project Plan.

8.2 The Supplier shall achieve Operational Acceptance of the System (or Subsystem(s) where a separate time for Operational Acceptance of such Subsystem(s) is specified in the Contract) in accordance with the time schedule specified in the Implementation Schedule and any refinements made in the Agreed Project Plan, or within such extended time to which the Supplier shall be entitled under GCC Clause 40 (Extension of Time for Achieving Operational Acceptance).

9. Supplier's Responsibilities

9.1 The Supplier shall conduct all activities with due care and diligence, in accordance with the Contract and with the skill and care expected of a competent provider of information technologies, information systems, support, maintenance, training, and other related services, or in accordance with best industry practices. In particular, the Supplier shall provide and employ only technical personnel who are skilled and experienced in their respective callings and supervisory staff who are competent to adequately supervise the work at hand.

9.2 The Supplier confirms that it has entered into this Contract on the basis of a proper examination of the data relating to the System provided by the Purchaser and on the basis of information that the Supplier could have obtained from a

visual inspection of the site (if access to the site was available) and of other data readily available to the Supplier relating to the System as at the date twenty-eight (28) days prior to bid submission. The Supplier acknowledges that any failure to acquaint itself with all such data and information shall not relieve its responsibility for properly estimating the difficulty or cost of successfully performing the Contract.

9.3 The Supplier shall be responsible for timely provision of all resources, information, and decision making under its control that are necessary to reach a mutually Agreed Project Plan (pursuant to GCC Clause 19.2) within the time schedule specified in the Implementation Schedule. Failure to provide such resources, information, and decision-making may constitute grounds for termination pursuant to GCC Clause 41.2.

9.4 The Supplier shall acquire in its name all permits, approvals, and/or licenses from all local, state, or national government authorities or public service undertakings in the Purchaser's Country that are necessary for the performance of the Contract, including, without limitation, visas for the Supplier's and Subcontractor's personnel and entry permits for all imported Supplier's Equipment. The Supplier shall acquire all other permits, approvals, and/or licenses that are not the responsibility of the Purchaser under GCC Clause 10.4 and that are necessary for the performance of the Contract.

9.5 The Supplier shall comply with all laws in force in the Purchaser's Country. The laws will include all national, provincial, municipal, or other laws that affect the performance of the Contract and are binding upon the Supplier. The Supplier shall indemnify and hold harmless the Purchaser from and against any and all liabilities, damages, claims, fines, penalties, and expenses of whatever nature arising or resulting from the violation of such laws by the Supplier or its personnel, including the Subcontractors and their personnel, but without prejudice to GCC Clause 10.1. The Supplier shall not indemnify the Purchaser to the extent that such liability, damage, claims, fines, penalties, and expenses were caused or contributed to by a fault of the Purchaser.

9.6 The Supplier shall, in all dealings with its labor and the labor of its Subcontractors currently employed on or connected with the Contract, pay due regard to all recognized festivals,

official holidays, religious or other customs, and all local laws and regulations pertaining to the employment of labor.

9.7 Any Information Technologies or other Goods and Services that will be incorporated in or be required for the System and other supplies shall have their Origin, as defined in GCC Clause 3.12, in a country that shall be an Eligible Country, as defined in GCC Clause 1.1 (e) (iv).

9.8 Pursuant to paragraph 2.2 e. of Appendix B to the General Conditions the Supplier shall permit and shall cause its subcontractors and subconsultants to permit, the Bank and/or persons appointed by the Bank to inspect the Site and/or the accounts and records relating to the performance of the Contract and the submission of the Bid, and to have such accounts and records audited by auditors appointed by the Bank if requested by the Bank. The Supplier's and its Subcontractors' and subconsultants' attention is drawn to Sub-Clause 6.1 which provides, inter alia, that acts intended to materially impede the exercise of the Bank's inspection and audit rights constitute a prohibited practice subject to contract termination (as well as to a determination of ineligibility pursuant to the Bank's prevailing sanctions procedures).

9.9 The Supplier shall conform to the sustainable procurement contractual provisions, if and as **specified in the SCC.**

9.10 **Unless otherwise specified in the SCC** the Supplier shall have no other Supplier responsibilities.

10. Purchaser's Responsibilities

10.1 The Purchaser shall ensure the accuracy of all information and/or data to be supplied by the Purchaser to the Supplier, except when otherwise expressly stated in the Contract.

10.2 The Purchaser shall be responsible for timely provision of all resources, information, and decision making under its control that are necessary to reach an Agreed Project Plan (pursuant to GCC Clause 19.2) within the time schedule specified in the Implementation Schedule. Failure to provide such resources, information, and decision making may constitute grounds for Termination pursuant to GCC Clause 41.3.1 (b).

10.3 The Purchaser shall be responsible for acquiring and providing legal and physical possession of the site and access to it, and for providing possession of and access to all other areas reasonably required for the proper execution of the Contract.

10.4 If requested by the Supplier, the Purchaser shall use its best endeavors to assist the Supplier in obtaining in a timely and expeditious manner all permits, approvals, and/or licenses necessary for the execution of the Contract from all local, state, or national government authorities or public service undertakings that such authorities or undertakings require the Supplier or Subcontractors or the personnel of the Supplier or Subcontractors, as the case may be, to obtain.

10.5 In such cases where the responsibilities of specifying and acquiring or upgrading telecommunications and/or electric power services falls to the Supplier, as specified in the Technical Requirements, SCC, Agreed Project Plan, or other parts of the Contract, the Purchaser shall use its best endeavors to assist the Supplier in obtaining such services in a timely and expeditious manner.

10.6 The Purchaser shall be responsible for timely provision of all resources, access, and information necessary for the Installation and Operational Acceptance of the System (including, but not limited to, any required telecommunications or electric power services), as identified in the Agreed Project Plan, except where provision of such items is explicitly identified in the Contract as being the responsibility of the Supplier. Delay by the Purchaser may result in an appropriate extension of the Time for Operational Acceptance, at the Supplier's discretion.

10.7 Unless otherwise specified in the Contract or agreed upon by the Purchaser and the Supplier, the Purchaser shall provide sufficient, properly qualified operating and technical personnel, as required by the Supplier to properly carry out Delivery, Pre-commissioning, Installation, Commissioning, and Operational Acceptance, at or before the time specified in the Implementation Schedule and the Agreed Project Plan.

10.8 The Purchaser will designate appropriate staff for the training courses to be given by the Supplier and shall make all appropriate logistical arrangements for such training as specified in the Technical Requirements, SCC, the Agreed Project Plan, or other parts of the Contract.

10.9 The Purchaser assumes primary responsibility for the Operational Acceptance Test(s) for the System, in accordance with GCC Clause 27.2, and shall be responsible for the continued operation of the System after Operational Acceptance. However, this shall not limit in any way the Supplier's responsibilities after the date of Operational

Acceptance otherwise specified in the Contract.

10.10 The Purchaser is responsible for performing and safely storing timely and regular backups of its data and Software in accordance with accepted data management principles, except where such responsibility is clearly assigned to the Supplier elsewhere in the Contract.

10.11 All costs and expenses involved in the performance of the obligations under this GCC Clause 10 shall be the responsibility of the Purchaser, save those to be incurred by the Supplier with respect to the performance of the Operational Acceptance Test(s), in accordance with GCC Clause 27.2.

10.12 **Unless otherwise specified in the SCC** the Purchaser shall have no other Purchaser responsibilities.

C. PAYMENT

11. Contract Price

11.1 The Contract Price shall be as specified in Article 2 (Contract Price and Terms of Payment) of the Contract Agreement.

11.2 The Contract Price shall be a firm lump sum not subject to any alteration, except:

(a) in the event of a Change in the System pursuant to GCC Clause 39 or to other clauses in the Contract;

(b) the price adjustment formula specified in the SCC (if any). **However, Unless otherwise specified in the SCC** there will NOT be a price adjustment formula**.**

11.3 The Supplier shall be deemed to have satisfied itself as to the correctness and sufficiency of the Contract Price, which shall, except as otherwise provided for in the Contract, cover all its obligations under the Contract.

12. Terms of Payment

12.1 The Supplier's request for payment shall be made to the Purchaser in writing, accompanied by an invoice describing, as appropriate, the System or Subsystem(s), Delivered, Pre-commissioned, Installed, and Operationally Accepted, and by documents submitted pursuant to GCC Clause 22.5 and upon fulfillment of other obligations stipulated in the Contract.

The Contract Price shall be paid as **specified in the SCC.**

12.2 No payment made by the Purchaser herein shall be deemed to constitute acceptance by the Purchaser of the System or any Subsystem(s).

12.3 Payments shall be made promptly by the Purchaser, but in no case later than forty five (45) days after submission of a valid invoice by the Supplier. In the event that the Purchaser fails to make any payment by its respective due date or within the period set forth in the Contract, the Purchaser shall pay to the Supplier interest on the amount of such delayed payment at the rate(s) **specified in the SCC** for the period of delay until payment has been made in full, whether before or after judgment or arbitration award.

12.4 Payments shall be made in the currency(ies) specified in the Contract Agreement, pursuant to GCC Clause 11. For Goods and Services supplied locally, payments shall be made **as specified in the SCC.**

12.5 **Unless otherwise specified in the SCC,** payment of the foreign currency portion of the Contract Price for Goods supplied from outside the Purchaser's Country shall be made to the Supplier through an irrevocable letter of credit opened by an authorized bank in the Supplier's Country and will be payable on presentation of the appropriate documents. It is agreed that the letter of credit will be subject to Article 10 of the latest revision of *Uniform Customs and Practice for Documentary Credits*, published by the International Chamber of Commerce, Paris.

13. Securities

13.1 Issuance of Securities

The Supplier shall provide the securities specified below in favor of the Purchaser at the times and in the amount, manner, and form specified below.

13.2 Advance Payment Security

13.2.1 The Supplier shall provide within twenty-eight (28)

days of the notification of Contract award an Advance Payment Security in the amount and currency of the Advance Payment specified in SCC for GCC Clause 12.1 above and valid until the System is Operationally Accepted.

13.2.2 The security shall be in the form provided in the bidding documents or in another form acceptable to the Purchaser. The amount of the security shall be reduced in proportion to the value of the System executed by and paid to the Supplier from time to time and shall automatically become null and void when the full amount of the advance payment has been recovered by the Purchaser. **Unless otherwise specified in the SCC,** the reduction in value and expiration of the Advance Payment Security are calculated as follows:

P*a/(100-a), where "P" is the sum of all payments effected so far to the Supplier (excluding the Advance Payment), and "a" is the Advance Payment expressed as a percentage of the Contract Price pursuant to the SCC for GCC Clause 12.1.

The security shall be returned to the Supplier immediately after its expiration.

13.3 Performance Security

13.3.1 The Supplier shall, within twenty-eight (28) days of the notification of Contract award, provide a security for the due performance of the Contract in the amount and currency **specified in the SCC.**

13.3.2 The security shall be a bank guarantee in the form provided in the Sample Contractual Forms Section of the bidding documents, or it shall be in another form acceptable to the Purchaser.

13.3.3 The security shall automatically become null and void once all the obligations of the Supplier under the Contract have been fulfilled, including, but not limited to, any obligations during the Warranty Period and any extensions to the period. The security shall be returned to the Supplier no later than twenty-eight (28) days after its expiration.

13.3.4 Upon Operational Acceptance of the entire System,

the security shall be reduced to the amount **specified in the SCC,** on the date of such Operational Acceptance, so that the reduced security would only cover the remaining warranty obligations of the Supplier.

14. Taxes and Duties

14.1 For Goods or Services supplied from outside the Purchaser's country, the Supplier shall be entirely responsible for all taxes, stamp duties, license fees, and other such levies imposed outside the Purchaser's country. Any duties, such as importation or customs duties, and taxes and other levies, payable in the Purchaser's country for the supply of Goods and Services from outside the Purchaser's country are the responsibility of the Purchaser unless these duties or taxes have been made part of the Contract Price in Article 2 of the Contract Agreement and the Price Schedule it refers to, in which case the duties and taxes will be the Supplier's responsibility.

14.2 For Goods or Services supplied locally, the Supplier shall be entirely responsible for all taxes, duties, license fees, etc., incurred until delivery of the contracted Goods or Services to the Purchaser. The only exception are taxes or duties, such as value-added or sales tax or stamp duty as apply to, or are clearly identifiable, on the invoices and provided they apply in the Purchaser's country, and only if these taxes, levies and/or duties are also excluded from the Contract Price in Article 2 of the Contract Agreement and the Price Schedule it refers to.

14.3 If any tax exemptions, reductions, allowances, or privileges may be available to the Supplier in the Purchaser's Country, the Purchaser shall use its best efforts to enable the Supplier to benefit from any such tax savings to the maximum allowable extent.

14.4 For the purpose of the Contract, it is agreed that the Contract Price specified in Article 2 (Contract Price and Terms of Payment) of the Contract Agreement is based on the taxes, duties, levies, and charges prevailing at the date twenty-eight (28) days prior to the date of bid submission in the Purchaser's Country (also called "Tax" in this GCC Clause 14.4). If any Tax rates are increased or decreased, a new Tax is introduced, an existing Tax is abolished, or any change in interpretation or application of any Tax occurs in the course of the performance of the Contract, which was or will be assessed on the Supplier, its Subcontractors, or their

employees in connection with performance of the Contract, an equitable adjustment to the Contract Price shall be made to fully take into account any such change by addition to or reduction from the Contract Price, as the case may be.

D. INTELLECTUAL PROPERTY

15. Copyright

15.1 The Intellectual Property Rights in all Standard Software and Standard Materials shall remain vested in the owner of such rights.

15.2 The Purchaser agrees to restrict use, copying, or duplication of the Standard Software and Standard Materials in accordance with GCC Clause 16, except that additional copies of Standard Materials may be made by the Purchaser for use within the scope of the project of which the System is a part, in the event that the Supplier does not deliver copies within thirty (30) days from receipt of a request for such Standard Materials.

15.3 The Purchaser's contractual rights to use the Standard Software or elements of the Standard Software may not be assigned, licensed, or otherwise transferred voluntarily except in accordance with the relevant license agreement or **unless otherwise specified in the SCC** to a legally constituted successor organization (e.g., a reorganization of a public entity formally authorized by the government or through a merger or acquisition of a private entity)**.**

15.4 **Unless otherwise specified in the SCC,** the Intellectual Property Rights in all Custom Software and Custom Materials specified in Appendices 4 and 5 of the Contract Agreement (if any) shall, at the date of this Contract or on creation of the rights (if later than the date of this Contract), vest in the Purchaser. The Supplier shall do and execute or arrange for the doing and executing of each necessary act, document, and thing that the Purchaser may consider necessary or desirable to perfect the right, title, and interest of the Purchaser in and to those rights. In respect of such Custom Software and Custom Materials, the Supplier shall ensure that the holder of a moral right in such an item does not assert it, and the Supplier shall, if requested to do so by the Purchaser and where permitted by applicable law, ensure that the holder of such a moral right waives it.

15.5 **Unless otherwise specified in the SCC**, escrow arrangements shall NOT be required.

16. Software License Agreements

16.1 Except to the extent that the Intellectual Property Rights in the Software vest in the Purchaser, the Supplier hereby grants to the Purchaser license to access and use the Software, including all inventions, designs, and marks embodied in the Software.

Such license to access and use the Software shall:

(a) be:

(i) nonexclusive;

(ii) fully paid up and irrevocable (except that it shall terminate if the Contract terminates under GCC Clauses 41.1 or 41.3);

(iii) **unless otherwise specified in the SCC** valid throughout the territory of the Purchaser's Country;

(iv) **unless otherwise specified in the SCC** subject to NO additional restrictions.

(b) permit the Software to be:

(i) used or copied for use on or with the computer(s) for which it was acquired (if specified in the Technical Requirements and/or the Supplier's bid), plus a backup computer(s) of the same or similar capacity, if the primary is(are) inoperative, and during a reasonable transitional period when use is being transferred between primary and backup;

(ii) used or copied for use on or transferred to a replacement computer(s), (and use on the original and replacement computer(s) may be simultaneous during a reasonable transitional period) provided that, if the Technical Requirements and/or the Supplier's bid specifies a class of computer to which the license is restricted, the replacement computer(s) is(are) within that class;

(iii) if the nature of the System is such as to permit such access, accessed from other computers

connected to the primary and/or backup computer(s) by means of a local or wide-area network or similar arrangement, and used on or copied for use on those other computers to the extent necessary to that access;

(iv) reproduced for safekeeping or backup purposes;

(v) customized, adapted, or combined with other computer software for use by the Purchaser, provided that derivative software incorporating any substantial part of the delivered, restricted Software shall be subject to same restrictions as are set forth in this Contract;

(vi) **unless otherwise specified in the SCC,** disclosed to, and reproduced for use by, support service suppliers and their subcontractors, (and the Purchaser may sublicense such persons to use and copy for use the Software) to the extent reasonably necessary to the performance of their support service contracts, subject to the same restrictions as are set forth in this Contract; and

(vii) **unless otherwise specified in the SCC** disclosed to, and reproduced for use by, NO other parties.

16.2 The Supplier has the right to audit the Standard Software to verify compliance with the above license agreements. **Unless otherwise specified in the SCC**, the Purchaser will make available to the Supplier, within seven (7) days of a written request, accurate and up-to-date records of the number and location of copies, the number of authorized users, or any other relevant data required to demonstrate use of the Standard Software as per the license agreement. If and only if, expressly agreed in writing between the Purchaser and the Supplier, Purchaser will allow, under a pre-specified agreed procedure, the execution of embedded software functions under Supplier's control, and unencumbered transmission of resulting information on software usage.

17. Confidential Information

17.1 **Unless otherwise specified in the SCC,** the "Receiving Party" (either the Purchaser or the Supplier) shall keep confidential and shall not, without the written consent of the other party to this Contract ("the Disclosing Party"), divulge to any third party any documents, data, or other information of a confidential nature ("Confidential Information") connected with this Contract, and furnished directly or indirectly by the Disclosing Party prior to or during performance, or following termination, of this Contract.

17.2 For the purposes of GCC Clause 17.1, the Supplier is also deemed to be the Receiving Party of Confidential Information generated by the Supplier itself in the course of the performance of its obligations under the Contract and relating to the businesses, finances, suppliers, employees, or other contacts of the Purchaser or the Purchaser's use of the System.

17.3 Notwithstanding GCC Clauses 17.1 and 17.2:

(a) the Supplier may furnish to its Subcontractor Confidential Information of the Purchaser to the extent reasonably required for the Subcontractor to perform its work under the Contract; and

(b) the Purchaser may furnish Confidential Information of the Supplier: (i) to its support service suppliers and their subcontractors to the extent reasonably required for them to perform their work under their support service contracts; and (ii) to its affiliates and subsidiaries,

in which event the Receiving Party shall ensure that the person to whom it furnishes Confidential Information of the Disclosing Party is aware of and abides by the Receiving Party's obligations under this GCC Clause 17 as if that person were party to the Contract in place of the Receiving Party.

17.4 The Purchaser shall not, without the Supplier's prior written consent, use any Confidential Information received from the Supplier for any purpose other than the operation, maintenance and further development of the System. Similarly, the Supplier shall not, without the Purchaser's prior written consent, use any Confidential Information received from the Purchaser for any purpose other than those that are required for the performance of the Contract.

17.5 The obligation of a party under GCC Clauses 17.1 through 17.4 above, however, shall not apply to that information which:

(a) now or hereafter enters the public domain through no fault of the Receiving Party;

(b) can be proven to have been possessed by the Receiving Party at the time of disclosure and that was not previously obtained, directly or indirectly, from the Disclosing Party;

(c) otherwise lawfully becomes available to the Receiving Party from a third party that has no obligation of confidentiality.

17.6 The above provisions of this GCC Clause 17 shall not in any way modify any undertaking of confidentiality given by either of the parties to this Contract prior to the date of the Contract in respect of the System or any part thereof.

17.7 **Unless otherwise specified in the SCC**, the provisions of this GCC Clause 17 shall survive the termination, for whatever reason, of the Contract for three (3) years.

E. SUPPLY, INSTALLATION, TESTING, COMMISSIONING, AND ACCEPTANCE OF THE SYSTEM

18. Representatives

18.1 Project Manager

If the Project Manager is not named in the Contract, then within fourteen (14) days of the Effective Date, the Purchaser shall appoint and notify the Supplier in writing of the name of the Project Manager. The Purchaser may from time to time appoint some other person as the Project Manager in place of the person previously so appointed and shall give a notice of the name of such other person to the Supplier without delay. No such appointment shall be made at such a time or in such a manner as to impede the progress of work on the System. Such appointment shall take effect only upon receipt of such notice by the Supplier. **Unless otherwise specified in the SCC** (if any), the Project Manager shall have the authority to represent the Purchaser on all day-to-day matters relating to the System or arising from the Contract, and shall normally be the person giving or receiving notices on behalf of the Purchaser pursuant to GCC

Clause 4.

18.2 Supplier's Representative

18.2.1 If the Supplier's Representative is not named in the Contract, then within fourteen (14) days of the Effective Date, the Supplier shall appoint the Supplier's Representative and shall request the Purchaser in writing to approve the person so appointed. The request must be accompanied by a detailed curriculum vitae for the nominee, as well as a description of any other System or non-System responsibilities the nominee would retain while performing the duties of the Supplier's Representative. If the Purchaser does not object to the appointment within fourteen (14) days, the Supplier's Representative shall be deemed to have been approved. If the Purchaser objects to the appointment within fourteen (14) days giving the reason therefor, then the Supplier shall appoint a replacement within fourteen (14) days of such objection in accordance with this GCC Clause 18.2.1.

18.2.2 **Unless otherwise specified in the SCC** (if any), the Supplier's Representative shall have the authority to represent the Supplier on all day-to-day matters relating to the System or arising from the Contract, and shall normally be the person giving or receiving notices on behalf of the Supplier pursuant to GCC Clause 4.

18.2.3 The Supplier shall not revoke the appointment of the Supplier's Representative without the Purchaser's prior written consent, which shall not be unreasonably withheld. If the Purchaser consents to such an action, the Supplier shall appoint another person of equal or superior qualifications as the Supplier's Representative, pursuant to the procedure set out in GCC Clause 18.2.1.

18.2.4 The Supplier's Representative and staff are obliged to work closely with the Purchaser's Project Manager and staff, act within their own authority, and abide by directives issued by the Purchaser that are consistent with the terms of the Contract. The Supplier's Representative is responsible for managing the activities of its personnel and any subcontracted

personnel.

18.2.5 The Supplier's Representative may, subject to the approval of the Purchaser (which shall not be unreasonably withheld), at any time delegate to any person any of the powers, functions, and authorities vested in him or her. Any such delegation may be revoked at any time. Any such delegation or revocation shall be subject to a prior notice signed by the Supplier's Representative and shall specify the powers, functions, and authorities thereby delegated or revoked. No such delegation or revocation shall take effect unless and until the notice of it has been delivered.

18.2.6 Any act or exercise by any person of powers, functions and authorities so delegated to him or her in accordance with GCC Clause 18.2.5 shall be deemed to be an act or exercise by the Supplier's Representative.

18.3 Objections and Removals

18.3.1 The Purchaser may by notice to the Supplier object to any representative or person employed by the Supplier in the execution of the Contract who, in the reasonable opinion of the Purchaser, may have behaved inappropriately, be incompetent, or be negligent. The Purchaser shall provide evidence of the same, whereupon the Supplier shall remove such person from work on the System.

18.3.2 If any representative or person employed by the Supplier is removed in accordance with GCC Clause 18.3.1, the Supplier shall, where required, promptly appoint a replacement.

19. Project Plan

19.1 In close cooperation with the Purchaser and based on the Preliminary Project Plan included in the Supplier's bid, the Supplier shall develop a Project Plan encompassing the activities specified in the Contract. The contents of the Project Plan shall be as **specified in the SCC** and/or Technical Requirements.

19.2 **Unless otherwise specified in the SCC**, within thirty (30) days from the Effective Date of the Contract, the Supplier shall present a Project Plan to the Purchaser. The Purchaser shall, within fourteen (14) days of receipt of the Project Plan,

notify the Supplier of any respects in which it considers that the Project Plan does not adequately ensure that the proposed program of work, proposed methods, and/or proposed Information Technologies will satisfy the Technical Requirements and/or the SCC (in this Clause 19.2 called "non-conformities" below). The Supplier shall, within five (5) days of receipt of such notification, correct the Project Plan and resubmit to the Purchaser. The Purchaser shall, within five (5) days of resubmission of the Project Plan, notify the Supplier of any remaining non-conformities. This procedure shall be repeated as necessary until the Project Plan is free from non-conformities. When the Project Plan is free from non-conformities, the Purchaser shall provide confirmation in writing to the Supplier. This approved Project Plan ("the Agreed Project Plan") shall be contractually binding on the Purchaser and the Supplier.

19.3 If required, the impact on the Implementation Schedule of modifications agreed during finalization of the Agreed Project Plan shall be incorporated in the Contract by amendment, in accordance with GCC Clauses 39 and 40.

19.4 The Supplier shall undertake to supply, install, test, and commission the System in accordance with the Agreed Project Plan and the Contract.

19.5 **Unless otherwise specified in the SCC**, the Supplier shall submit to the Purchaser Monthly Progress Reports summarizing:

(i) results accomplished during the prior period;

(ii) cumulative deviations to date from schedule of progress milestones as specified in the Agreed Project Plan;

(iii) corrective actions to be taken to return to planned schedule of progress; proposed revisions to planned schedule;

(iv) other issues and outstanding problems; proposed actions to be taken;

(v) resources that the Supplier expects to be provided by the Purchaser and/or actions to be taken by the Purchaser in the next reporting period;

(vi) other issues or potential problems the Supplier foresees that could impact on project progress and/or

effectiveness.

19.6 The Supplier shall submit to the Purchaser other (periodic) reports **as specified in the SCC**.

20. Subcontracting

20.1 Appendix 3 (List of Approved Subcontractors) to the Contract Agreement specifies critical items of supply or services and a list of Subcontractors for each item that are considered acceptable by the Purchaser. If no Subcontractors are listed for an item, the Supplier shall prepare a list of Subcontractors it considers qualified and wishes to be added to the list for such items. The Supplier may from time to time propose additions to or deletions from any such list. The Supplier shall submit any such list or any modification to the list to the Purchaser for its approval in sufficient time so as not to impede the progress of work on the System. The Purchaser shall not withhold such approval unreasonably. Such approval by the Purchaser of a Subcontractor(s) shall not relieve the Supplier from any of its obligations, duties, or responsibilities under the Contract.

20.2 The Supplier may, at its discretion, select and employ Subcontractors for such critical items from those Subcontractors listed pursuant to GCC Clause 20.1. If the Supplier wishes to employ a Subcontractor not so listed, or subcontract an item not so listed, it must seek the Purchaser's prior approval under GCC Clause 20.3.

20.3 For items for which pre-approved Subcontractor lists have not been specified in Appendix 3 to the Contract Agreement, the Supplier may employ such Subcontractors as it may select, provided: (i) the Supplier notifies the Purchaser in writing at least twenty-eight (28) days prior to the proposed mobilization date for such Subcontractor; and (ii) by the end of this period either the Purchaser has granted its approval in writing or fails to respond. The Supplier shall not engage any Subcontractor to which the Purchaser has objected in writing prior to the end of the notice period. The absence of a written objection by the Purchaser during the above specified period shall constitute formal acceptance of the proposed Subcontractor. Except to the extent that it permits the deemed approval of the Purchaser of Subcontractors not listed in the Contract Agreement, nothing in this Clause, however, shall limit the rights and obligations of either the Purchaser or Supplier as they are specified in GCC Clauses 20.1 and 20.2, or in Appendix 3 of the Contract

Agreement.

21. Design and Engineering

21.1 Technical Specifications and Drawings

21.1.1 The Supplier shall execute the basic and detailed design and the implementation activities necessary for successful installation of the System in compliance with the provisions of the Contract or, where not so specified, in accordance with good industry practice.

The Supplier shall be responsible for any discrepancies, errors or omissions in the specifications, drawings, and other technical documents that it has prepared, whether such specifications, drawings, and other documents have been approved by the Project Manager or not, provided that such discrepancies, errors, or omissions are not because of inaccurate information furnished in writing to the Supplier by or on behalf of the Purchaser.

21.1.2 The Supplier shall be entitled to disclaim responsibility for any design, data, drawing, specification, or other document, or any modification of such design, drawings, specification, or other documents provided or designated by or on behalf of the Purchaser, by giving a notice of such disclaimer to the Project Manager.

21.2 Codes and Standards

Wherever references are made in the Contract to codes and standards in accordance with which the Contract shall be executed, the edition or the revised version of such codes and standards current at the date twenty-eight (28) days prior to date of bid submission shall apply. During Contract execution, any changes in such codes and standards shall be applied after approval by the Purchaser and shall be treated in accordance with GCC Clause 39.3.

21.3 Approval/Review of Controlling Technical Documents by the Project Manager

21.3.1 **Unless otherwise specified in the SCC**, there will NO Controlling Technical Documents required. However, **if the SCC specifies** Controlling Technical Documents, the Supplier shall prepare and furnish such documents for the Project Manager's approval or

review.

Any part of the System covered by or related to the documents to be approved by the Project Manager shall be executed only after the Project Manager's approval of these documents.

GCC Clauses 21.3.2 through 21.3.7 shall apply to those documents requiring the Project Manager's approval, but not to those furnished to the Project Manager for its review only.

21.3.2 Within fourteen (14) days after receipt by the Project Manager of any document requiring the Project Manager's approval in accordance with GCC Clause 21.3.1, the Project Manager shall either return one copy of the document to the Supplier with its approval endorsed on the document or shall notify the Supplier in writing of its disapproval of the document and the reasons for disapproval and the modifications that the Project Manager proposes. If the Project Manager fails to take such action within the fourteen (14) days, then the document shall be deemed to have been approved by the Project Manager.

21.3.3 The Project Manager shall not disapprove any document except on the grounds that the document does not comply with some specified provision of the Contract or that it is contrary to good industry practice.

21.3.4 If the Project Manager disapproves the document, the Supplier shall modify the document and resubmit it for the Project Manager's approval in accordance with GCC Clause 21.3.2. If the Project Manager approves the document subject to modification(s), the Supplier shall make the required modification(s), and the document shall then be deemed to have been approved, subject to GCC Clause 21.3.5. The procedure set out in GCC Clauses 21.3.2 through 21.3.4 shall be repeated, as appropriate, until the Project Manager approves such documents.

21.3.5 If any dispute occurs between the Purchaser and the Supplier in connection with or arising out of the disapproval by the Project Manager of any document and/or any modification(s) to a document that cannot be settled between the parties within a reasonable

period, then, in case the Contract Agreement includes and names an Adjudicator, such dispute may be referred to the Adjudicator for determination in accordance with GCC Clause 6.1 (Adjudicator). If such dispute is referred to an Adjudicator, the Project Manager shall give instructions as to whether and if so, how, performance of the Contract is to proceed. The Supplier shall proceed with the Contract in accordance with the Project Manager's instructions, provided that if the Adjudicator upholds the Supplier's view on the dispute and if the Purchaser has not given notice under GCC Clause 6.1.2, then the Supplier shall be reimbursed by the Purchaser for any additional costs incurred by reason of such instructions and shall be relieved of such responsibility or liability in connection with the dispute and the execution of the instructions as the Adjudicator shall decide, and the Time for Achieving Operational Acceptance shall be extended accordingly.

21.3.6 The Project Manager's approval, with or without modification of the document furnished by the Supplier, shall not relieve the Supplier of any responsibility or liability imposed upon it by any provisions of the Contract except to the extent that any subsequent failure results from modifications required by the Project Manager or inaccurate information furnished in writing to the Supplier by or on behalf of the Purchaser.

21.3.7 The Supplier shall not depart from any approved document unless the Supplier has first submitted to the Project Manager an amended document and obtained the Project Manager's approval of the document, pursuant to the provisions of this GCC Clause 21.3. If the Project Manager requests any change in any already approved document and/or in any document based on such an approved document, the provisions of GCC Clause 39 (Changes to the System) shall apply to such request.

22. Procurement, Delivery, and Transport

22.1 Subject to related Purchaser's responsibilities pursuant to GCC Clauses 10 and 14, the Supplier shall manufacture or procure and transport all the Information Technologies, Materials, and other Goods in an expeditious and orderly

manner to the Project Site.

22.2 Delivery of the Information Technologies, Materials, and other Goods shall be made by the Supplier in accordance with the Technical Requirements.

22.3 Early or partial deliveries require the explicit written consent of the Purchaser, which consent shall not be unreasonably withheld.

22.4 Transportation

22.4.1 The Supplier shall provide such packing of the Goods as is required to prevent their damage or deterioration during shipment. The packing, marking, and documentation within and outside the packages shall comply strictly with the Purchaser's instructions to the Supplier.

22.4.2 The Supplier will bear responsibility for and cost of transport to the Project Sites in accordance with the terms and conditions used in the specification of prices in the Price Schedules, including the terms and conditions of the associated Incoterms.

22.4.3 **Unless otherwise specified in the SCC,** the Supplier shall be free to use transportation through carriers registered in any eligible country and to obtain insurance from any eligible source country.

22.5 **Unless otherwise specified in the SCC,** the Supplier will provide the Purchaser with shipping and other documents, as specified below:

22.5.1 For Goods supplied from outside the Purchaser's Country:

Upon shipment, the Supplier shall notify the Purchaser and the insurance company contracted by the Supplier to provide cargo insurance by telex, cable, facsimile, electronic mail, or EDI with the full details of the shipment. The Supplier shall promptly send the following documents to the Purchaser by mail or courier, as appropriate, with a copy to the cargo insurance company:

(a) two copies of the Supplier's invoice showing the description of the Goods, quantity, unit price, and

total amount;

(b) usual transportation documents;

(c) insurance certificate;

(d) certificate(s) of origin; and

(e) estimated time and point of arrival in the Purchaser's Country and at the site.

22.5.2 For Goods supplied locally (i.e., from within the Purchaser's country):

Upon shipment, the Supplier shall notify the Purchaser by telex, cable, facsimile, electronic mail, or EDI with the full details of the shipment. The Supplier shall promptly send the following documents to the Purchaser by mail or courier, as appropriate:

(a) two copies of the Supplier's invoice showing the Goods' description, quantity, unit price, and total amount;

(b) delivery note, railway receipt, or truck receipt;

(c) certificate of insurance;

(d) certificate(s) of origin; and

(e) estimated time of arrival at the site.

22.6 Customs Clearance

(a) The Purchaser will bear responsibility for, and cost of, customs clearance into the Purchaser's country in accordance the particular Incoterm(s) used for Goods supplied from outside the Purchaser's country in the Price Schedules referred to by Article 2 of the Contract Agreement.

(b) At the request of the Purchaser, the Supplier will make available a representative or agent during the process of customs clearance in the Purchaser's country for goods supplied from outside the Purchaser's country. In the event of delays in customs clearance that are not the fault of the Supplier:

(i) the Supplier shall be entitled to an extension in the Time for Achieving Operational Acceptance,

pursuant to GCC Clause 40;

(ii) the Contract Price shall be adjusted to compensate the Supplier for any additional storage charges that the Supplier may incur as a result of the delay.

23. Product Upgrades

23.1 At any point during performance of the Contract, should technological advances be introduced by the Supplier for Information Technologies originally offered by the Supplier in its bid and still to be delivered, the Supplier shall be obligated to offer to the Purchaser the latest versions of the available Information Technologies having equal or better performance or functionality at the same or lesser unit prices, pursuant to GCC Clause 39 (Changes to the System).

23.2 At any point during performance of the Contract, for Information Technologies still to be delivered, the Supplier will also pass on to the Purchaser any cost reductions and additional and/or improved support and facilities that it offers to other clients of the Supplier in the Purchaser's Country, pursuant to GCC Clause 39 (Changes to the System).

23.3 During performance of the Contract, the Supplier shall offer to the Purchaser all new versions, releases, and updates of Standard Software, as well as related documentation and technical support services, within thirty (30) days of their availability from the Supplier to other clients of the Supplier in the Purchaser's Country, and no later than twelve (12) months after they are released in the country of origin. In no case will the prices for these Software exceed those quoted by the Supplier in the Recurrent Costs tables in its bid.

23.4 **Unless otherwise specified in the SCC,** during the Warranty Period, the Supplier will provide at no additional cost to the Purchaser all new versions, releases, and updates for all Standard Software that are used in the System, within thirty (30) days of their availability from the Supplier to other clients of the Supplier in the Purchaser's country, and no later than twelve (12) months after they are released in the country of origin of the Software.

23.5 The Purchaser shall introduce all new versions, releases or updates of the Software within eighteen (18) months of receipt of a production-ready copy of the new version, release, or update, provided that the new version, release, or update does not adversely affect System operation or

performance or require extensive reworking of the System. In cases where the new version, release, or update adversely affects System operation or performance, or requires extensive reworking of the System, the Supplier shall continue to support and maintain the version or release previously in operation for as long as necessary to allow introduction of the new version, release, or update. In no case shall the Supplier stop supporting or maintaining a version or release of the Software less than twenty four (24) months after the Purchaser receives a production-ready copy of a subsequent version, release, or update. The Purchaser shall use all reasonable endeavors to implement any new version, release, or update as soon as practicable, subject to the twenty-four-month-long stop date.

24. Implementation, Installation, and Other Services

24.1 The Supplier shall provide all Services specified in the Contract and Agreed Project Plan in accordance with the highest standards of professional competence and integrity.

24.2 Prices charged by the Supplier for Services, if not included in the Contract, shall be agreed upon in advance by the parties (including, but not restricted to, any prices submitted by the Supplier in the Recurrent Cost Schedules of its Bid) and shall not exceed the prevailing rates charged by the Supplier to other purchasers in the Purchaser's Country for similar services.

25. Inspections and Tests

25.1 The Purchaser or its representative shall have the right to inspect and/or test any components of the System, as specified in the Technical Requirements, to confirm their good working order and/or conformity to the Contract at the point of delivery and/or at the Project Site.

25.2 The Purchaser or its representative shall be entitled to attend any such inspections and/or tests of the components, provided that the Purchaser shall bear all costs and expenses incurred in connection with such attendance, including but not limited to all inspection agent fees, travel, and related expenses.

25.3 Should the inspected or tested components fail to conform to the Contract, the Purchaser may reject the component(s), and the Supplier shall either replace the rejected component(s), or make alterations as necessary so that it meets the Contract requirements free of cost to the Purchaser.

25.4 The Project Manager may require the Supplier to carry out any inspection and/or test not specified in the Contract,

provided that the Supplier's reasonable costs and expenses incurred in the carrying out of such inspection and/or test shall be added to the Contract Price. Further, if such inspection and/or test impedes the progress of work on the System and/or the Supplier's performance of its other obligations under the Contract, due allowance will be made in respect of the Time for Achieving Operational Acceptance and the other obligations so affected.

25.5 If any dispute shall arise between the parties in connection with or caused by an inspection and/or with regard to any component to be incorporated in the System that cannot be settled amicably between the parties within a reasonable period of time, either party may invoke the process pursuant to GCC Clause 43 (Settlement of Disputes), starting with referral of the matter to the Adjudicator in case an Adjudicator is included and named in the Contract Agreement.

26. Installation of the System

26.1 As soon as the System, or any Subsystem, has, in the opinion of the Supplier, been delivered, Pre-commissioned, and made ready for Commissioning and Operational Acceptance Testing in accordance with the Technical Requirements, the SCC and the Agreed Project Plan, the Supplier shall so notify the Purchaser in writing.

26.2 The Project Manager shall, within fourteen (14) days after receipt of the Supplier's notice under GCC Clause 26.1, either issue an Installation Certificate in the form specified in the Sample Contractual Forms Section in the bidding documents, stating that the System, or major component or Subsystem (if Acceptance by major component or Subsystem is specified pursuant to the SCC for GCC Clause 27.2.1), has achieved Installation by the date of the Supplier's notice under GCC Clause 26.1, or notify the Supplier in writing of any defects and/or deficiencies, including, but not limited to, defects or deficiencies in the interoperability or integration of the various components and/or Subsystems making up the System. The Supplier shall use all reasonable endeavors to promptly remedy any defect and/or deficiencies that the Project Manager has notified the Supplier of. The Supplier shall then promptly carry out retesting of the System or Subsystem and, when in the Supplier's opinion the System or Subsystem is ready for Commissioning and Operational Acceptance Testing, notify the Purchaser in writing, in accordance with GCC Clause 26.1. The procedure set out in this GCC Clause 26.2

shall be repeated, as necessary, until an Installation Certificate is issued.

26.3 If the Project Manager fails to issue the Installation Certificate and fails to inform the Supplier of any defects and/or deficiencies within fourteen (14) days after receipt of the Supplier's notice under GCC Clause 26.1, or if the Purchaser puts the System or a Subsystem into production operation, then the System (or Subsystem) shall be deemed to have achieved successful Installation as of the date of the Supplier's notice or repeated notice, or when the Purchaser put the System into production operation, as the case may be.

27. Commissioning and Operational Acceptance

27.1 Commissioning

27.1.1 Commissioning of the System (or Subsystem if specified pursuant to the SCC for GCC Clause 27.2.1) shall be commenced by the Supplier:

(a) immediately after the Installation Certificate is issued by the Project Manager, pursuant to GCC Clause 26.2; or

(b) as otherwise specified in the Technical Requirement or the Agreed Project Plan; or

(c) immediately after Installation is deemed to have occurred, under GCC Clause 26.3.

27.1.2 The Purchaser shall supply the operating and technical personnel and all materials and information reasonably required to enable the Supplier to carry out its obligations with respect to Commissioning.

Production use of the System or Subsystem(s) shall not commence prior to the start of formal Operational Acceptance Testing.

27.2 Operational Acceptance Tests

27.2.1 The Operational Acceptance Tests (and repeats of such tests) shall be the primary responsibility of the Purchaser (in accordance with GCC Clause 10.9), but shall be conducted with the full cooperation of the Supplier during Commissioning of the System (or major components or Subsystem[s]), to ascertain whether the System (or major component or Subsystem[s]) conforms to the Technical Requirements and meets the standard of performance

quoted in the Supplier's bid, including, but not restricted to, the functional and technical performance requirements. **Unless otherwise specified in the SCC**, the Operational Acceptance Tests during Commissioning will be conducted as specified in the Technical Requirements and/or the Agreed Project Plan.

At the Purchaser's discretion, Operational Acceptance Tests may also be performed on replacement Goods, upgrades and new version releases, and Goods that are added or field-modified after Operational Acceptance of the System.

27.2.2 If for reasons attributable to the Purchaser, the Operational Acceptance Test of the System (or Subsystem[s] or major components, pursuant to the SCC for GCC Clause 27.2.1) cannot be successfully completed within ninety (90) days from the date of Installation or any other period agreed upon in writing by the Purchaser and the Supplier, the Supplier shall be deemed to have fulfilled its obligations with respect to the technical and functional aspects of the Technical Specifications, SCC and/or the Agreed Project Plan, and GCC Clause 28.2 and 28.3 shall not apply.

27.3 Operational Acceptance

27.3.1 Subject to GCC Clause 27.4 (Partial Acceptance) below, Operational Acceptance shall occur in respect of the System, when

(a) the Operational Acceptance Tests, as specified in the Technical Requirements, and/or SCC and/or the Agreed Project Plan have been successfully completed; or

(b) the Operational Acceptance Tests have not been successfully completed or have not been carried out for reasons that are attributable to the Purchaser within the period from the date of Installation or any other agreed-upon period as specified in GCC Clause 27.2.2 above; or

(c) the Purchaser has put the System into production or use for sixty (60) consecutive days. If the System is put into production or use in this

manner, the Supplier shall notify the Purchaser and document such use.

27.3.2 At any time after any of the events set out in GCC Clause 27.3.1 have occurred, the Supplier may give a notice to the Project Manager requesting the issue of an Operational Acceptance Certificate.

27.3.3 After consultation with the Purchaser, and within fourteen (14) days after receipt of the Supplier's notice, the Project Manager shall:

(a) issue an Operational Acceptance Certificate; or

(b) notify the Supplier in writing of any defect or deficiencies or other reason for the failure of the Operational Acceptance Tests; or

(c) issue the Operational Acceptance Certificate, if the situation covered by GCC Clause 27.3.1 (b) arises.

27.3.4 The Supplier shall use all reasonable endeavors to promptly remedy any defect and/or deficiencies and/or other reasons for the failure of the Operational Acceptance Test that the Project Manager has notified the Supplier of. Once such remedies have been made by the Supplier, the Supplier shall notify the Purchaser, and the Purchaser, with the full cooperation of the Supplier, shall use all reasonable endeavors to promptly carry out retesting of the System or Subsystem. Upon the successful conclusion of the Operational Acceptance Tests, the Supplier shall notify the Purchaser of its request for Operational Acceptance Certification, in accordance with GCC Clause 27.3.3. The Purchaser shall then issue to the Supplier the Operational Acceptance Certification in accordance with GCC Clause 27.3.3 (a), or shall notify the Supplier of further defects, deficiencies, or other reasons for the failure of the Operational Acceptance Test. The procedure set out in this GCC Clause 27.3.4 shall be repeated, as necessary, until an Operational Acceptance Certificate is issued.

27.3.5 If the System or Subsystem fails to pass the Operational Acceptance Test(s) in accordance with GCC Clause 27.2, then either:

(a) the Purchaser may consider terminating the Contract, pursuant to GCC Clause 41.2.2;

or

(b) if the failure to achieve Operational Acceptance within the specified time period is a result of the failure of the Purchaser to fulfill its obligations under the Contract, then the Supplier shall be deemed to have fulfilled its obligations with respect to the relevant technical and functional aspects of the Contract, and GCC Clauses 30.3 and 30.4 shall not apply.

27.3.6 If within fourteen (14) days after receipt of the Supplier's notice the Project Manager fails to issue the Operational Acceptance Certificate or fails to inform the Supplier in writing of the justifiable reasons why the Project Manager has not issued the Operational Acceptance Certificate, the System or Subsystem shall be deemed to have been accepted as of the date of the Supplier's said notice.

27.4 Partial Acceptance

27.4.1 If so specified in the SCC for GCC Clause 27.2.1, Installation and Commissioning shall be carried out individually for each identified major component or Subsystem(s) of the System. In this event, the provisions in the Contract relating to Installation and Commissioning, including the Operational Acceptance Test, shall apply to each such major component or Subsystem individually, and Operational Acceptance Certificate(s) shall be issued accordingly for each such major component or Subsystem of the System, subject to the limitations contained in GCC Clause 27.4.2.

27.4.2 The issuance of Operational Acceptance Certificates for individual major components or Subsystems pursuant to GCC Clause 27.4.1 shall not relieve the Supplier of its obligation to obtain an Operational Acceptance Certificate for the System as an integrated whole (if so specified in the SCC for GCC Clauses 12.1 and 27.2.1) once all major components and Subsystems have been supplied, installed, tested, and commissioned.

27.4.3 In the case of minor components for the System that by their nature do not require Commissioning or an Operational Acceptance Test (e.g., minor fittings,

furnishings or site works, etc.), the Project Manager shall issue an Operational Acceptance Certificate within fourteen (14) days after the fittings and/or furnishings have been delivered and/or installed or the site works have been completed. The Supplier shall, however, use all reasonable endeavors to promptly remedy any defects or deficiencies in such minor components detected by the Purchaser or Supplier.

F. GUARANTEES AND LIABILITIES

28. Operational Acceptance Time Guarantee

28.1 The Supplier guarantees that it shall complete the supply, Installation, Commissioning, and achieve Operational Acceptance of the System (or Subsystems, pursuant to the SCC for GCC Clause 27.2.1) within the time periods specified in the Implementation Schedule and/or the Agreed Project Plan pursuant to GCC Clause 8.2, or within such extended time to which the Supplier shall be entitled under GCC Clause 40 (Extension of Time for Achieving Operational Acceptance).

28.2 **Unless otherwise specified in the SCC**, if the Supplier fails to supply, install, commission, and achieve Operational Acceptance of the System (or Subsystems pursuant to the SCC for GCC Clause 27.2.1) within the time for achieving Operational Acceptance specified in the Implementation Schedule or the Agreed Project Plan, or any extension of the time for achieving Operational Acceptance previously granted under GCC Clause 40 (Extension of Time for Achieving Operational Acceptance), the Supplier shall pay to the Purchaser liquidated damages at the rate of one half of one percent per week as a percentage of the Contract Price (exclusive of Recurrent Costs if any), or the relevant part of the Contract Price if a Subsystem has not achieved Operational Acceptance. The aggregate amount of such liquidated damages shall in no event exceed the amount of ten (10) percent of the Contract Price (exclusive of Recurrent Costs if any). Once the Maximum is reached, the Purchaser may consider termination of the Contract, pursuant to GCC Clause 41.2.2.

28.3 **Unless otherwise specified in the SCC,** liquidated damages payable under GCC Clause 28.2 shall apply only to the failure to achieve Operational Acceptance of the System (and Subsystems) as specified in the Implementation Schedule and/or Agreed Project Plan. This Clause 28.3 shall not limit, however, any other rights or remedies the

Purchaser may have under the Contract for other delays.

28.4 If liquidated damages are claimed by the Purchaser for the System (or Subsystem), the Supplier shall have no further liability whatsoever to the Purchaser in respect to the Operational Acceptance time guarantee for the System (or Subsystem). However, the payment of liquidated damages shall not in any way relieve the Supplier from any of its obligations to complete the System or from any other of its obligations and liabilities under the Contract.

29. Defect Liability

29.1 The Supplier warrants that the System, including all Information Technologies, Materials, and other Goods supplied and Services provided, shall be free from defects in the design, engineering, Materials, and workmanship that prevent the System and/or any of its components from fulfilling the Technical Requirements or that limit in a material fashion the performance, reliability, or extensibility of the System and/or Subsystems. **Unless otherwise specified in the SCC**, there will be NO exceptions and/or limitations to this warranty with respect to Software (or categories of Software). Commercial warranty provisions of products supplied under the Contract shall apply to the extent that they do not conflict with the provisions of this Contract.

29.2 The Supplier also warrants that the Information Technologies, Materials, and other Goods supplied under the Contract are new, unused, and incorporate all recent improvements in design that materially affect the System's or Subsystem's ability to fulfill the Technical Requirements.

29.3 **Unless otherwise specified in the SCC,** the Supplier warrants that: (i) all Goods components to be incorporated into the System form part of the Supplier's and/or Subcontractor's current product lines, and (ii) they have been previously released to the market.

29.4 **Unless otherwise specified in the SCC**, the Warranty Period shall commence from the date of Operational Acceptance of the System (or of any major component or Subsystem for which separate Operational Acceptance is provided for in the Contract) and shall extend for thirty-six (36) months.

29.5 If during the Warranty Period any defect as described in GCC Clause 29.1 should be found in the design, engineering, Materials, and workmanship of the Information

Technologies and other Goods supplied or of the Services provided by the Supplier, the Supplier shall promptly, in consultation and agreement with the Purchaser regarding appropriate remedying of the defects, and at its sole cost, repair, replace, or otherwise make good (as the Supplier shall, at its discretion, determine) such defect as well as any damage to the System caused by such defect. Any defective Information Technologies or other Goods that have been replaced by the Supplier shall remain the property of the Supplier.

29.6 The Supplier shall not be responsible for the repair, replacement, or making good of any defect, or of any damage to the System arising out of or resulting from any of the following causes:

(a) improper operation or maintenance of the System by the Purchaser;

(b) normal wear and tear;

(c) use of the System with items not supplied by the Supplier, unless otherwise identified in the Technical Requirements, or approved by the Supplier; or

(d) modifications made to the System by the Purchaser, or a third party, not approved by the Supplier.

29.7 The Supplier's obligations under this GCC Clause 29 shall not apply to:

(a) any materials that are normally consumed in operation or have a normal life shorter than the Warranty Period; or

(b) any designs, specifications, or other data designed, supplied, or specified by or on behalf of the Purchaser or any matters for which the Supplier has disclaimed responsibility, in accordance with GCC Clause 21.1.2.

29.8 The Purchaser shall give the Supplier a notice promptly following the discovery of such defect, stating the nature of any such defect together with all available evidence. The Purchaser shall afford all reasonable opportunity for the Supplier to inspect any such defect. The Purchaser shall afford the Supplier all necessary access to the System and the site to enable the Supplier to perform its obligations under this GCC Clause 29.

29.9 The Supplier may, with the consent of the Purchaser, remove

from the site any Information Technologies and other Goods that are defective, if the nature of the defect, and/or any damage to the System caused by the defect, is such that repairs cannot be expeditiously carried out at the site. If the repair, replacement, or making good is of such a character that it may affect the efficiency of the System, the Purchaser may give the Supplier notice requiring that tests of the defective part be made by the Supplier immediately upon completion of such remedial work, whereupon the Supplier shall carry out such tests.

If such part fails the tests, the Supplier shall carry out further repair, replacement, or making good (as the case may be) until that part of the System passes such tests. The tests shall be agreed upon by the Purchaser and the Supplier.

29.10 **Unless otherwise specified in the SCC**, the response times and repair/replacement times for Warranty Defect Repair are specified in the Technical Requirements. Nevertheless, if the Supplier fails to commence the work necessary to remedy such defect or any damage to the System caused by such defect within two weeks the Purchaser may, following notice to the Supplier, proceed to do such work or contract a third party (or parties) to do such work, and the reasonable costs incurred by the Purchaser in connection with such work shall be paid to the Purchaser by the Supplier or may be deducted by the Purchaser from any monies due the Supplier or claimed under the Performance Security.

29.11 If the System or Subsystem cannot be used by reason of such defect and/or making good of such defect, the Warranty Period for the System shall be extended by a period equal to the period during which the System or Subsystem could not be used by the Purchaser because of such defect and/or making good of such defect.

29.12 Items substituted for defective parts of the System during the Warranty Period shall be covered by the Defect Liability Warranty for the remainder of the Warranty Period applicable for the part replaced or three (3) months, whichever is greater. For reasons of information security, the Purchaser may choose to retain physical possession of any replaced defective information storage devices.

29.13 At the request of the Purchaser and without prejudice to any other rights and remedies that the Purchaser may have against the Supplier under the Contract, the Supplier will

offer all possible assistance to the Purchaser to seek warranty services or remedial action from any subcontracted third-party producers or licensor of Goods included in the System, including without limitation assignment or transfer in favor of the Purchaser of the benefit of any warranties given by such producers or licensors to the Supplier.

30. Functional Guarantees

30.1 The Supplier guarantees that, once the Operational Acceptance Certificate(s) has been issued, the System represents a complete, integrated solution to the Purchaser's requirements set forth in the Technical Requirements and it conforms to all other aspects of the Contract. The Supplier acknowledges that GCC Clause 27 regarding Commissioning and Operational Acceptance governs how technical conformance of the System to the Contract requirements will be determined.

30.2 If, for reasons attributable to the Supplier, the System does not conform to the Technical Requirements or does not conform to all other aspects of the Contract, the Supplier shall at its cost and expense make such changes, modifications, and/or additions to the System as may be necessary to conform to the Technical Requirements and meet all functional and performance standards. The Supplier shall notify the Purchaser upon completion of the necessary changes, modifications, and/or additions and shall request the Purchaser to repeat the Operational Acceptance Tests until the System achieves Operational Acceptance.

30.3 If the System (or Subsystem[s]) fails to achieve Operational Acceptance, the Purchaser may consider termination of the Contract, pursuant to GCC Clause 41.2.2, and forfeiture of the Supplier's Performance Security in accordance with GCC Clause 13.3 in compensation for the extra costs and delays likely to result from this failure.

31. Intellectual Property Rights Warranty

31.1 The Supplier hereby represents and warrants that:

(a) the System as supplied, installed, tested, and accepted;

(b) use of the System in accordance with the Contract; and

(c) copying of the Software and Materials provided to the Purchaser in accordance with the Contract

do not and will not infringe any Intellectual Property Rights held by any third party and that it has all necessary rights or at its sole expense shall have secured in writing all transfers

of rights and other consents necessary to make the assignments, licenses, and other transfers of Intellectual Property Rights and the warranties set forth in the Contract, and for the Purchaser to own or exercise all Intellectual Property Rights as provided in the Contract. Without limitation, the Supplier shall secure all necessary written agreements, consents, and transfers of rights from its employees and other persons or entities whose services are used for development of the System.

32. Intellectual Property Rights Indemnity

32.1 The Supplier shall indemnify and hold harmless the Purchaser and its employees and officers from and against any and all losses, liabilities, and costs (including losses, liabilities, and costs incurred in defending a claim alleging such a liability), that the Purchaser or its employees or officers may suffer as a result of any infringement or alleged infringement of any Intellectual Property Rights by reason of:

(a) installation of the System by the Supplier or the use of the System, including the Materials, in the country where the site is located;

(b) copying of the Software and Materials provided the Supplier in accordance with the Agreement; and

(c) sale of the products produced by the System in any country, except to the extent that such losses, liabilities, and costs arise as a result of the Purchaser's breach of GCC Clause 32.2.

32.2 Such indemnity shall not cover any use of the System, including the Materials, other than for the purpose indicated by or to be reasonably inferred from the Contract, any infringement resulting from the use of the System, or any products of the System produced thereby in association or combination with any other goods or services not supplied by the Supplier, where the infringement arises because of such association or combination and not because of use of the System in its own right.

32.3 Such indemnities shall also not apply if any claim of infringement:

(a) is asserted by a parent, subsidiary, or affiliate of the Purchaser's organization;

(b) is a direct result of a design mandated by the

Purchaser's Technical Requirements and the possibility of such infringement was duly noted in the Supplier's Bid; or

(c) results from the alteration of the System, including the Materials, by the Purchaser or any persons other than the Supplier or a person authorized by the Supplier.

32.4 If any proceedings are brought or any claim is made against the Purchaser arising out of the matters referred to in GCC Clause 32.1, the Purchaser shall promptly give the Supplier notice of such proceedings or claims, and the Supplier may at its own expense and in the Purchaser's name conduct such proceedings or claim and any negotiations for the settlement of any such proceedings or claim.

If the Supplier fails to notify the Purchaser within twenty-eight (28) days after receipt of such notice that it intends to conduct any such proceedings or claim, then the Purchaser shall be free to conduct the same on its own behalf. Unless the Supplier has so failed to notify the Purchaser within the twenty-eight (28) days, the Purchaser shall make no admission that may be prejudicial to the defense of any such proceedings or claim. The Purchaser shall, at the Supplier's request, afford all available assistance to the Supplier in conducting such proceedings or claim and shall be reimbursed by the Supplier for all reasonable expenses incurred in so doing.

32.5 The Purchaser shall indemnify and hold harmless the Supplier and its employees, officers, and Subcontractors from and against any and all losses, liabilities, and costs (including losses, liabilities, and costs incurred in defending a claim alleging such a liability) that the Supplier or its employees, officers, or Subcontractors may suffer as a result of any infringement or alleged infringement of any Intellectual Property Rights arising out of or in connection with any design, data, drawing, specification, or other documents or materials provided to the Supplier in connection with this Contract by the Purchaser or any persons (other than the Supplier) contracted by the Purchaser, except to the extent that such losses, liabilities, and costs arise as a result of the Supplier's breach of GCC Clause 32.8.

32.6 Such indemnity shall not cover

(a) any use of the design, data, drawing, specification, or

other documents or materials, other than for the purpose indicated by or to be reasonably inferred from the Contract;

(b) any infringement resulting from the use of the design, data, drawing, specification, or other documents or materials, or any products produced thereby, in association or combination with any other Goods or Services not provided by the Purchaser or any other person contracted by the Purchaser, where the infringement arises because of such association or combination and not because of the use of the design, data, drawing, specification, or other documents or materials in its own right.

32.7 Such indemnities shall also not apply:

(a) if any claim of infringement is asserted by a parent, subsidiary, or affiliate of the Supplier's organization;

(b) to the extent that any claim of infringement is caused by the alteration, by the Supplier, or any persons contracted by the Supplier, of the design, data, drawing, specification, or other documents or materials provided to the Supplier by the Purchaser or any persons contracted by the Purchaser.

32.8 If any proceedings are brought or any claim is made against the Supplier arising out of the matters referred to in GCC Clause 32.5, the Supplier shall promptly give the Purchaser notice of such proceedings or claims, and the Purchaser may at its own expense and in the Supplier's name conduct such proceedings or claim and any negotiations for the settlement of any such proceedings or claim. If the Purchaser fails to notify the Supplier within twenty-eight (28) days after receipt of such notice that it intends to conduct any such proceedings or claim, then the Supplier shall be free to conduct the same on its own behalf. Unless the Purchaser has so failed to notify the Supplier within the twenty-eight (28) days, the Supplier shall make no admission that may be prejudicial to the defense of any such proceedings or claim. The Supplier shall, at the Purchaser's request, afford all available assistance to the Purchaser in conducting such proceedings or claim and shall be reimbursed by the Purchaser for all reasonable expenses incurred in so doing.

33. Limitation of Liability

33.1 Provided the following does not exclude or limit any liabilities of either party in ways not permitted by applicable law:

(a) the Supplier shall not be liable to the Purchaser, whether in contract, tort, or otherwise, for any indirect or consequential loss or damage, loss of use, loss of production, or loss of profits or interest costs, provided that this exclusion shall not apply to any obligation of the Supplier to pay liquidated damages to the Purchaser; and

(b) the aggregate liability of the Supplier to the Purchaser, whether under the Contract, in tort or otherwise, shall not exceed the total Contract Price, provided that this limitation shall not apply to any obligation of the Supplier to indemnify the Purchaser with respect to intellectual property rights infringement.

G. RISK DISTRIBUTION

34. Transfer of Ownership

34.1 With the exception of Software and Materials, the ownership of the Information Technologies and other Goods shall be transferred to the Purchaser at the time of Delivery or otherwise under terms that may be agreed upon and specified in the Contract Agreement.

34.2 Ownership and the terms of usage of the Software and Materials supplied under the Contract shall be governed by GCC Clause 15 (Copyright) and any elaboration in the Technical Requirements.

34.3 Ownership of the Supplier's Equipment used by the Supplier and its Subcontractors in connection with the Contract shall remain with the Supplier or its Subcontractors.

35. Care of the System

35.1 The Purchaser shall become responsible for the care and custody of the System or Subsystems upon their Delivery. The Purchaser shall make good at its own cost any loss or damage that may occur to the System or Subsystems from any cause from the date of Delivery until the date of Operational Acceptance of the System or Subsystems, pursuant to GCC Clause 27 (Commissioning and Operational Acceptance), excepting such loss or damage arising from acts or omissions of the Supplier, its employees, or subcontractors.

35.2 If any loss or damage occurs to the System or any part of the System by reason of:

(a) (insofar as they relate to the country where the Project Site is located) nuclear reaction, nuclear radiation, radioactive contamination, a pressure wave caused by aircraft or other aerial objects, or any other occurrences that an experienced contractor could not reasonably foresee, or if reasonably foreseeable could not reasonably make provision for or insure against, insofar as such risks are not normally insurable on the insurance market and are mentioned in the general exclusions of the policy of insurance taken out under GCC Clause 37;

(b) any use not in accordance with the Contract, by the Purchaser or any third party;

(c) any use of or reliance upon any design, data, or specification provided or designated by or on behalf of the Purchaser, or any such matter for which the Supplier has disclaimed responsibility in accordance with GCC Clause 21.1.2,

the Purchaser shall pay to the Supplier all sums payable in respect of the System or Subsystems that have achieved Operational Acceptance, notwithstanding that the same be lost, destroyed, or damaged. If the Purchaser requests the Supplier in writing to make good any loss or damage to the System thereby occasioned, the Supplier shall make good the same at the cost of the Purchaser in accordance with GCC Clause 39. If the Purchaser does not request the Supplier in writing to make good any loss or damage to the System thereby occasioned, the Purchaser shall either request a change in accordance with GCC Clause 39, excluding the performance of that part of the System thereby lost, destroyed, or damaged, or, where the loss or damage affects a substantial part of the System, the Purchaser shall terminate the Contract pursuant to GCC Clause 41.1.

35.3 The Purchaser shall be liable for any loss of or damage to any Supplier's Equipment which the Purchaser has authorized to locate within the Purchaser's premises for use in fulfillment of Supplier's obligations under the Contract, except where such loss or damage arises from acts or omissions of the Supplier, its employees, or subcontractors.

36. Loss of or Damage to Property; Accident or Injury to Workers; Indemnification

36.1 The Supplier and each and every Subcontractor shall abide by the job safety, insurance, customs, and immigration measures prevalent and laws in force in the Purchaser's Country.

36.2 Subject to GCC Clause 36.3, the Supplier shall indemnify and hold harmless the Purchaser and its employees and officers from and against any and all losses, liabilities and costs (including losses, liabilities, and costs incurred in defending a claim alleging such a liability) that the Purchaser or its employees or officers may suffer as a result of the death or injury of any person or loss of or damage to any property (other than the System, whether accepted or not) arising in connection with the supply, installation, testing, and Commissioning of the System and by reason of the negligence of the Supplier or its Subcontractors, or their employees, officers or agents, except any injury, death, or property damage caused by the negligence of the Purchaser, its contractors, employees, officers, or agents.

36.3 If any proceedings are brought or any claim is made against the Purchaser that might subject the Supplier to liability under GCC Clause 36.2, the Purchaser shall promptly give the Supplier notice of such proceedings or claims, and the Supplier may at its own expense and in the Purchaser's name conduct such proceedings or claim and any negotiations for the settlement of any such proceedings or claim. If the Supplier fails to notify the Purchaser within twenty-eight (28) days after receipt of such notice that it intends to conduct any such proceedings or claim, then the Purchaser shall be free to conduct the same on its own behalf. Unless the Supplier has so failed to notify the Purchaser within the twenty-eight (28) day period, the Purchaser shall make no admission that may be prejudicial to the defense of any such proceedings or claim. The Purchaser shall, at the Supplier's request, afford all available assistance to the Supplier in conducting such proceedings or claim and shall be reimbursed by the Supplier for all reasonable expenses incurred in so doing.

36.4 The Purchaser shall indemnify and hold harmless the Supplier and its employees, officers, and Subcontractors from any and all losses, liabilities, and costs (including losses, liabilities, and costs incurred in defending a claim alleging such a liability) that the Supplier or its employees, officers, or Subcontractors may suffer as a result of the death or personal injury of any person or loss of or damage to

property of the Purchaser, other than the System not yet achieving Operational Acceptance, that is caused by fire, explosion, or any other perils, in excess of the amount recoverable from insurances procured under GCC Clause 37 (Insurances), provided that such fire, explosion, or other perils were not caused by any act or failure of the Supplier.

36.5 If any proceedings are brought or any claim is made against the Supplier that might subject the Purchaser to liability under GCC Clause 36.4, the Supplier shall promptly give the Purchaser notice of such proceedings or claims, and the Purchaser may at its own expense and in the Supplier's name conduct such proceedings or claim and any negotiations for the settlement of any such proceedings or claim. If the Purchaser fails to notify the Supplier within twenty-eight (28) days after receipt of such notice that it intends to conduct any such proceedings or claim, then the Supplier shall be free to conduct the same on its own behalf. Unless the Purchaser has so failed to notify the Supplier within the twenty-eight (28) days, the Supplier shall make no admission that may be prejudicial to the defense of any such proceedings or claim. The Supplier shall, at the Purchaser's request, afford all available assistance to the Purchaser in conducting such proceedings or claim and shall be reimbursed by the Purchaser for all reasonable expenses incurred in so doing.

36.6 The party entitled to the benefit of an indemnity under this GCC Clause 36 shall take all reasonable measures to mitigate any loss or damage that has occurred. If the party fails to take such measures, the other party's liabilities shall be correspondingly reduced.

37. Insurances

37.1 The Supplier shall at its expense take out and maintain in effect, or cause to be taken out and maintained in effect, during the performance of the Contract, the insurance set forth below. The identity of the insurers and the form of the policies shall be subject to the approval of the Purchaser, who should not unreasonably withhold such approval.

(a) Cargo Insurance During Transport

as applicable, 110 percent of the price of the Information Technologies and other Goods in a freely convertible currency, covering the Goods from physical loss or damage during shipment through receipt at the Project Site.

(b) Installation "All Risks" Insurance

as applicable, 110 percent of the price of the Information Technologies and other Goods covering the Goods at the site from all risks of physical loss or damage (excluding only perils commonly excluded under "all risks" insurance policies of this type by reputable insurers) occurring prior to Operational Acceptance of the System.

(c) Third-Party Liability Insurance

On terms as **specified in the SCC,** covering bodily injury or death suffered by third parties (including the Purchaser's personnel) and loss of or damage to property (including the Purchaser's property and any Subsystems that have been accepted by the Purchaser) occurring in connection with the supply and installation of the Information System.

(d) Automobile Liability Insurance

In accordance with the statutory requirements prevailing in the Purchaser's Country, covering use of all vehicles used by the Supplier or its Subcontractors (whether or not owned by them) in connection with the execution of the Contract.

(e) Other Insurance (if any), as **specified in the SCC.**

37.2 The Purchaser shall be named as co-insured under all insurance policies taken out by the Supplier pursuant to GCC Clause 37.1, except for the Third-Party Liability, and the Supplier's Subcontractors shall be named as co-insured under all insurance policies taken out by the Supplier pursuant to GCC Clause 37.1 except for Cargo Insurance During Transport. All insurer's rights of subrogation against such co-insured for losses or claims arising out of the performance of the Contract shall be waived under such policies.

37.3 The Supplier shall deliver to the Purchaser certificates of insurance (or copies of the insurance policies) as evidence that the required policies are in full force and effect.

37.4 The Supplier shall ensure that, where applicable, its Subcontractor(s) shall take out and maintain in effect adequate insurance policies for their personnel and vehicles and for work executed by them under the Contract, unless

such Subcontractors are covered by the policies taken out by the Supplier.

37.5 If the Supplier fails to take out and/or maintain in effect the insurance referred to in GCC Clause 37.1, the Purchaser may take out and maintain in effect any such insurance and may from time to time deduct from any amount due the Supplier under the Contract any premium that the Purchaser shall have paid to the insurer or may otherwise recover such amount as a debt due from the Supplier.

37.6 Unless otherwise provided in the Contract, the Supplier shall prepare and conduct all and any claims made under the policies affected by it pursuant to this GCC Clause 37, and all monies payable by any insurers shall be paid to the Supplier. The Purchaser shall give to the Supplier all such reasonable assistance as may be required by the Supplier in connection with any claim under the relevant insurance policies. With respect to insurance claims in which the Purchaser's interest is involved, the Supplier shall not give any release or make any compromise with the insurer without the prior written consent of the Purchaser. With respect to insurance claims in which the Supplier's interest is involved, the Purchaser shall not give any release or make any compromise with the insurer without the prior written consent of the Supplier.

38. Force Majeure

38.1 "Force Majeure" shall mean any event beyond the reasonable control of the Purchaser or of the Supplier, as the case may be, and which is unavoidable notwithstanding the reasonable care of the party affected and shall include, without limitation, the following:

(a) war, hostilities, or warlike operations (whether a state of war be declared or not), invasion, act of foreign enemy, and civil war;

(b) rebellion, revolution, insurrection, mutiny, usurpation of civil or military government, conspiracy, riot, civil commotion, and terrorist acts;

(c) confiscation, nationalization, mobilization, commandeering or requisition by or under the order of any government or de jure or de facto authority or ruler, or any other act or failure to act of any local state or national government authority;

(d) strike, sabotage, lockout, embargo, import restriction,

port congestion, lack of usual means of public transportation and communication, industrial dispute, shipwreck, shortage or restriction of power supply, epidemics, quarantine, and plague;

(e) earthquake, landslide, volcanic activity, fire, flood or inundation, tidal wave, typhoon or cyclone, hurricane, storm, lightning, or other inclement weather condition, nuclear and pressure waves, or other natural or physical disaster;

(f) failure, by the Supplier, to obtain the necessary export permit(s) from the governments of the Country(s) of Origin of the Information Technologies or other Goods, or Supplier's Equipment provided that the Supplier has made all reasonable efforts to obtain the required export permit(s), including the exercise of due diligence in determining the eligibility of the System and all of its components for receipt of the necessary export permits.

38.2 If either party is prevented, hindered, or delayed from or in performing any of its obligations under the Contract by an event of Force Majeure, then it shall notify the other in writing of the occurrence of such event and the circumstances of the event of Force Majeure within fourteen (14) days after the occurrence of such event.

38.3 The party who has given such notice shall be excused from the performance or punctual performance of its obligations under the Contract for so long as the relevant event of Force Majeure continues and to the extent that such party's performance is prevented, hindered, or delayed. The Time for Achieving Operational Acceptance shall be extended in accordance with GCC Clause 40 (Extension of Time for Achieving Operational Acceptance).

38.4 The party or parties affected by the event of Force Majeure shall use reasonable efforts to mitigate the effect of the event of Force Majeure upon its or their performance of the Contract and to fulfill its or their obligations under the Contract, but without prejudice to either party's right to terminate the Contract under GCC Clause 38.6.

38.5 No delay or nonperformance by either party to this Contract caused by the occurrence of any event of Force Majeure shall:

(a) constitute a default or breach of the Contract;

(b) (subject to GCC Clauses 35.2, 38.3, and 38.4) give rise to any claim for damages or additional cost or expense occasioned by the delay or nonperformance,

if, and to the extent that, such delay or nonperformance is caused by the occurrence of an event of Force Majeure.

38.6 If the performance of the Contract is substantially prevented, hindered, or delayed for a single period of more than sixty (60) days or an aggregate period of more than one hundred and twenty (120) days on account of one or more events of Force Majeure during the time period covered by the Contract, the parties will attempt to develop a mutually satisfactory solution, failing which, either party may terminate the Contract by giving a notice to the other.

38.7 In the event of termination pursuant to GCC Clause 38.6, the rights and obligations of the Purchaser and the Supplier shall be as specified in GCC Clauses 41.1.2 and 41.1.3.

38.8 Notwithstanding GCC Clause 38.5, Force Majeure shall not apply to any obligation of the Purchaser to make payments to the Supplier under this Contract.

H. CHANGE IN CONTRACT ELEMENTS

39. Changes to the System

39.1 Introducing a Change

39.1.1 Subject to GCC Clauses 39.2.5 and 39.2.7, the Purchaser shall have the right to propose, and subsequently require, the Project Manager to order the Supplier from time to time during the performance of the Contract to make any change, modification, addition, or deletion to, in, or from the System (interchangeably called "Change"), provided that such Change falls within the general scope of the System, does not constitute unrelated work, and is technically practicable, taking into account both the state of advancement of the System and the technical compatibility of the Change envisaged with the nature of the System as originally specified in the Contract.

A Change may involve, but is not restricted to, the substitution of updated Information Technologies

and related Services in accordance with GCC Clause 23 (Product Upgrades).

39.1.2 The Supplier may from time to time during its performance of the Contract propose to the Purchaser (with a copy to the Project Manager) any Change that the Supplier considers necessary or desirable to improve the quality or efficiency of the System. The Purchaser may at its discretion approve or reject any Change proposed by the Supplier.

39.1.3 Notwithstanding GCC Clauses 39.1.1 and 39.1.2, no change made necessary because of any default of the Supplier in the performance of its obligations under the Contract shall be deemed to be a Change, and such change shall not result in any adjustment of the Contract Price or the Time for Achieving Operational Acceptance.

39.1.4 The procedure on how to proceed with and execute Changes is specified in GCC Clauses 39.2 and 39.3, and further details and sample forms are provided in the Sample Contractual Forms Section in the bidding documents.

39.1.5 Moreover, the Purchaser and Supplier will agree, during development of the Project Plan, to a date prior to the scheduled date for Operational Acceptance, after which the Technical Requirements for the System shall be "frozen." Any Change initiated after this time will be dealt with after Operational Acceptance.

39.2 Changes Originating from Purchaser

39.2.1 If the Purchaser proposes a Change pursuant to GCC Clauses 39.1.1, it shall send to the Supplier a "Request for Change Proposal," requiring the Supplier to prepare and furnish to the Project Manager as soon as reasonably practicable a "Change Proposal," which shall include the following:

(a) brief description of the Change;

(b) impact on the Time for Achieving Operational Acceptance;

(c) detailed estimated cost of the Change;

(d) effect on Functional Guarantees (if any);

(e) effect on any other provisions of the Contract.

39.2.2 Prior to preparing and submitting the "Change Proposal," the Supplier shall submit to the Project Manager a "Change Estimate Proposal," which shall be an estimate of the cost of preparing the Change Proposal, plus a first approximation of the suggested approach and cost for implementing the changes. Upon receipt of the Supplier's Change Estimate Proposal, the Purchaser shall do one of the following:

(a) accept the Supplier's estimate with instructions to the Supplier to proceed with the preparation of the Change Proposal;

(b) advise the Supplier of any part of its Change Estimate Proposal that is unacceptable and request the Supplier to review its estimate;

(c) advise the Supplier that the Purchaser does not intend to proceed with the Change.

39.2.3 Upon receipt of the Purchaser's instruction to proceed under GCC Clause 39.2.2 (a), the Supplier shall, with proper expedition, proceed with the preparation of the Change Proposal, in accordance with GCC Clause 39.2.1. The Supplier, at its discretion, may specify a validity period for the Change Proposal, after which if the Purchaser and Supplier has not reached agreement in accordance with GCC Clause 39.2.6, then GCC Clause 39.2.7 shall apply.

39.2.4 The pricing of any Change shall, as far as practicable, be calculated in accordance with the rates and prices included in the Contract. If the nature of the Change is such that the Contract rates and prices are inequitable, the parties to the Contract shall agree on other specific rates to be used for valuing the Change.

39.2.5 If before or during the preparation of the Change Proposal it becomes apparent that the aggregate impact of compliance with the Request for Change

Proposal and with all other Change Orders that have already become binding upon the Supplier under this GCC Clause 39 would be to increase or decrease the Contract Price as originally set forth in Article 2 (Contract Price) of the Contract Agreement by more than fifteen (15) percent, the Supplier may give a written notice of objection to this Request for Change Proposal prior to furnishing the Change Proposal. If the Purchaser accepts the Supplier's objection, the Purchaser shall withdraw the proposed Change and shall notify the Supplier in writing of its acceptance.

The Supplier's failure to so object to a Request for Change Proposal shall neither affect its right to object to any subsequent requested Changes or Change Orders, nor affect its right to take into account, when making such subsequent objection, the percentage increase or decrease in the Contract Price that any Change not objected to by the Supplier represents.

39.2.6 Upon receipt of the Change Proposal, the Purchaser and the Supplier shall mutually agree upon all matters contained in the Change Proposal. Within fourteen (14) days after such agreement, the Purchaser shall, if it intends to proceed with the Change, issue the Supplier a Change Order. If the Purchaser is unable to reach a decision within fourteen (14) days, it shall notify the Supplier with details of when the Supplier can expect a decision. If the Purchaser decides not to proceed with the Change for whatever reason, it shall, within the said period of fourteen (14) days, notify the Supplier accordingly. Under such circumstances, the Supplier shall be entitled to reimbursement of all costs reasonably incurred by it in the preparation of the Change Proposal, provided that these do not exceed the amount given by the Supplier in its Change Estimate Proposal submitted in accordance with GCC Clause 39.2.2.

39.2.7 If the Purchaser and the Supplier cannot reach agreement on the price for the Change, an equitable adjustment to the Time for Achieving Operational Acceptance, or any other matters identified in the Change Proposal, the Change will not be

implemented. However, this provision does not limit the rights of either party under GCC Clause 6 (Settlement of Disputes).

39.3 Changes Originating from Supplier

If the Supplier proposes a Change pursuant to GCC Clause 39.1.2, the Supplier shall submit to the Project Manager a written "Application for Change Proposal," giving reasons for the proposed Change and including the information specified in GCC Clause 39.2.1. Upon receipt of the Application for Change Proposal, the parties shall follow the procedures outlined in GCC Clauses 39.2.6 and 39.2.7. However, should the Purchaser choose not to proceed or the Purchaser and the Supplier cannot come to agreement on the change during any validity period that the Supplier may specify in its Application for Change Proposal, the Supplier shall not be entitled to recover the costs of preparing the Application for Change Proposal, unless subject to an agreement between the Purchaser and the Supplier to the contrary.

39.4 Value engineering. The Supplier may prepare, at its own cost, a value engineering proposal at any time during the performance of the Contract. The value engineering proposal shall, at a minimum, include the following;

(a) the proposed change(s), and a description of the difference to the existing Contract requirements;

(b) a full cost/benefit analysis of the proposed change(s) including a description and estimate of costs (including life cycle costs) the Purchaser may incur in implementing the value engineering proposal; and

(c) a description of any effect(s) of the change on performance/functionality.

The Purchaser may accept the value engineering proposal if the proposal demonstrates benefits that:

(a) accelerates the delivery period; or

(b) reduces the Contract Price or the life cycle costs to the Purchaser; or

(c) improves the quality, efficiency, safety or sustainability of the systems; or

(d) yields any other benefits to the Purchaser,

without compromising the necessary functions of the systems.

If the value engineering proposal is approved by the Purchaser and results in:

(a) a reduction of the Contract Price; the amount to be paid to the Supplier shall be the percentage specified in the SCC of the reduction in the Contract Price; or

(b) an increase in the Contract Price; but results in a reduction in life cycle costs due to any benefit described in (a) to (d) above, the amount to be paid to the Supplier shall be the full increase in the Contract Price.

40. Extension of Time for Achieving Operational Acceptance

40.1 The time(s) for achieving Operational Acceptance specified in the Schedule of Implementation shall be extended if the Supplier is delayed or impeded in the performance of any of its obligations under the Contract by reason of any of the following:

(a) any Change in the System as provided in GCC Clause 39 (Change in the Information System);

(b) any occurrence of Force Majeure as provided in GCC Clause 38 (Force Majeure);

(c) default of the Purchaser; or

(d) any other matter specifically mentioned in the Contract;

by such period as shall be fair and reasonable in all the circumstances and as shall fairly reflect the delay or impediment sustained by the Supplier.

40.2 Except where otherwise specifically provided in the Contract, the Supplier shall submit to the Project Manager a notice of a claim for an extension of the time for achieving Operational Acceptance, together with particulars of the event or circumstance justifying such extension as soon as reasonably practicable after the commencement of such

event or circumstance. As soon as reasonably practicable after receipt of such notice and supporting particulars of the claim, the Purchaser and the Supplier shall agree upon the period of such extension. In the event that the Supplier does not accept the Purchaser's estimate of a fair and reasonable time extension, the Supplier shall be entitled to refer the matter to the provisions for the Settlement of Disputes pursuant to GCC Clause 6.

40.3 The Supplier shall at all times use its reasonable efforts to minimize any delay in the performance of its obligations under the Contract.

41. Termination

41.1 Termination for Purchaser's Convenience

41.1.1 The Purchaser may at any time terminate the Contract for any reason by giving the Supplier a notice of termination that refers to this GCC Clause 41.1.

41.1.2 Upon receipt of the notice of termination under GCC Clause 41.1.1, the Supplier shall either as soon as reasonably practical or upon the date specified in the notice of termination

(a) cease all further work, except for such work as the Purchaser may specify in the notice of termination for the sole purpose of protecting that part of the System already executed, or any work required to leave the site in a clean and safe condition;

(b) terminate all subcontracts, except those to be assigned to the Purchaser pursuant to GCC Clause 41.1.2 (d) (ii) below;

(c) remove all Supplier's Equipment from the site, repatriate the Supplier's and its Subcontractors' personnel from the site, remove from the site any wreckage, rubbish, and debris of any kind;

(d) in addition, the Supplier, subject to the payment specified in GCC Clause 41.1.3, shall

(i) deliver to the Purchaser the parts of the System executed by the Supplier up to the date of termination;

(ii) to the extent legally possible, assign to the

Purchaser all right, title, and benefit of the Supplier to the System, or Subsystem, as at the date of termination, and, as may be required by the Purchaser, in any subcontracts concluded between the Supplier and its Subcontractors;

(iii) deliver to the Purchaser all nonproprietary drawings, specifications, and other documents prepared by the Supplier or its Subcontractors as of the date of termination in connection with the System.

41.1.3 In the event of termination of the Contract under GCC Clause 41.1.1, the Purchaser shall pay to the Supplier the following amounts:

(a) the Contract Price, properly attributable to the parts of the System executed by the Supplier as of the date of termination;

(b) the costs reasonably incurred by the Supplier in the removal of the Supplier's Equipment from the site and in the repatriation of the Supplier's and its Subcontractors' personnel;

(c) any amount to be paid by the Supplier to its Subcontractors in connection with the termination of any subcontracts, including any cancellation charges;

(d) costs incurred by the Supplier in protecting the System and leaving the site in a clean and safe condition pursuant to GCC Clause 41.1.2 (a); and

(e) the cost of satisfying all other obligations, commitments, and claims that the Supplier may in good faith have undertaken with third parties in connection with the Contract and that are not covered by GCC Clauses 41.1.3 (a) through (d) above.

41.2 Termination for Supplier's Default

41.2.1 The Purchaser, without prejudice to any other rights or remedies it may possess, may terminate the Contract forthwith in the following circumstances by giving a notice of termination and its reasons therefore to the Supplier, referring

to this GCC Clause 41.2:

(a) if the Supplier becomes bankrupt or insolvent, has a receiving order issued against it, compounds with its creditors, or, if the Supplier is a corporation, a resolution is passed or order is made for its winding up (other than a voluntary liquidation for the purposes of amalgamation or reconstruction), a receiver is appointed over any part of its undertaking or assets, or if the Supplier takes or suffers any other analogous action in consequence of debt;

(b) if the Supplier assigns or transfers the Contract or any right or interest therein in violation of the provision of GCC Clause 42 (Assignment); or

(c) if the Supplier, in the judgment of the Purchaser has engaged in Fraud and Corruption, as defined in paragraph 2.2 a. of the Appendix to the GCC, in competing for or in executing the Contract, including but not limited to willful misrepresentation of facts concerning ownership of Intellectual Property Rights in, or proper authorization and/or licenses from the owner to offer, the hardware, software, or materials provided under this Contract.

41.2.2 If the Supplier:

(a) has abandoned or repudiated the Contract;

(b) has without valid reason failed to commence work on the System promptly;

(c) persistently fails to execute the Contract in accordance with the Contract or persistently neglects to carry out its obligations under the Contract without just cause;

(d) refuses or is unable to provide sufficient Materials, Services, or labor to execute and complete the System in the manner specified in the Agreed Project Plan furnished under GCC Clause 19 at rates of progress that give reasonable assurance to the Purchaser that the Supplier can attain Operational Acceptance of the System by the Time for Achieving

Operational Acceptance as extended;

then the Purchaser may, without prejudice to any other rights it may possess under the Contract, give a notice to the Supplier stating the nature of the default and requiring the Supplier to remedy the same. If the Supplier fails to remedy or to take steps to remedy the same within fourteen (14) days of its receipt of such notice, then the Purchaser may terminate the Contract forthwith by giving a notice of termination to the Supplier that refers to this GCC Clause 41.2.

41.2.3 Upon receipt of the notice of termination under GCC Clauses 41.2.1 or 41.2.2, the Supplier shall, either immediately or upon such date as is specified in the notice of termination:

(a) cease all further work, except for such work as the Purchaser may specify in the notice of termination for the sole purpose of protecting that part of the System already executed or any work required to leave the site in a clean and safe condition;

(b) terminate all subcontracts, except those to be assigned to the Purchaser pursuant to GCC Clause 41.2.3 (d) below;

(c) deliver to the Purchaser the parts of the System executed by the Supplier up to the date of termination;

(d) to the extent legally possible, assign to the Purchaser all right, title and benefit of the Supplier to the System or Subsystems as at the date of termination, and, as may be required by the Purchaser, in any subcontracts concluded between the Supplier and its Subcontractors;

(e) deliver to the Purchaser all drawings, specifications, and other documents prepared by the Supplier or its Subcontractors as at the date of termination in connection with the System.

41.2.4 The Purchaser may enter upon the site, expel the Supplier, and complete the System itself or by employing any third party. Upon completion of the

System or at such earlier date as the Purchaser thinks appropriate, the Purchaser shall give notice to the Supplier that such Supplier's Equipment will be returned to the Supplier at or near the site and shall return such Supplier's Equipment to the Supplier in accordance with such notice. The Supplier shall thereafter without delay and at its cost remove or arrange removal of the same from the site.

41.2.5 Subject to GCC Clause 41.2.6, the Supplier shall be entitled to be paid the Contract Price attributable to the portion of the System executed as at the date of termination and the costs, if any, incurred in protecting the System and in leaving the site in a clean and safe condition pursuant to GCC Clause 41.2.3 (a). Any sums due the Purchaser from the Supplier accruing prior to the date of termination shall be deducted from the amount to be paid to the Supplier under this Contract.

41.2.6 If the Purchaser completes the System, the cost of completing the System by the Purchaser shall be determined. If the sum that the Supplier is entitled to be paid, pursuant to GCC Clause 41.2.5, plus the reasonable costs incurred by the Purchaser in completing the System, exceeds the Contract Price, the Supplier shall be liable for such excess. If such excess is greater than the sums due the Supplier under GCC Clause 41.2.5, the Supplier shall pay the balance to the Purchaser, and if such excess is less than the sums due the Supplier under GCC Clause 41.2.5, the Purchaser shall pay the balance to the Supplier. The Purchaser and the Supplier shall agree, in writing, on the computation described above and the manner in which any sums shall be paid.

41.3 Termination by Supplier

41.3.1 If:

(a) the Purchaser has failed to pay the Supplier any sum due under the Contract within the specified period, has failed to approve any invoice or supporting documents without just cause **pursuant to the SCC,** or commits a substantial breach of the Contract, the Supplier may give a notice to the Purchaser that requires payment of

such sum, with interest on this sum as stipulated in GCC Clause 12.3, requires approval of such invoice or supporting documents, or specifies the breach and requires the Purchaser to remedy the same, as the case may be. If the Purchaser fails to pay such sum together with such interest, fails to approve such invoice or supporting documents or give its reasons for withholding such approval, fails to remedy the breach or take steps to remedy the breach within fourteen (14) days after receipt of the Supplier's notice; or

(b) the Supplier is unable to carry out any of its obligations under the Contract for any reason attributable to the Purchaser, including but not limited to the Purchaser's failure to provide possession of or access to the site or other areas or failure to obtain any governmental permit necessary for the execution and/or completion of the System;

then the Supplier may give a notice to the Purchaser of such events, and if the Purchaser has failed to pay the outstanding sum, to approve the invoice or supporting documents, to give its reasons for withholding such approval, or to remedy the breach within twenty-eight (28) days of such notice, or if the Supplier is still unable to carry out any of its obligations under the Contract for any reason attributable to the Purchaser within twenty-eight (28) days of the said notice, the Supplier may by a further notice to the Purchaser referring to this GCC Clause 41.3.1, forthwith terminate the Contract.

41.3.2 The Supplier may terminate the Contract immediately by giving a notice to the Purchaser to that effect, referring to this GCC Clause 41.3.2, if the Purchaser becomes bankrupt or insolvent, has a receiving order issued against it, compounds with its creditors, or, being a corporation, if a resolution is passed or order is made for its winding up (other than a voluntary liquidation for the purposes of amalgamation or reconstruction), a receiver is appointed over any part of its undertaking or assets, or if the Purchaser takes or suffers any other analogous action in consequence of debt.

41.3.3 If the Contract is terminated under GCC Clauses 41.3.1 or 41.3.2, then the Supplier shall immediately:

(a) cease all further work, except for such work as may be necessary for the purpose of protecting that part of the System already executed, or any work required to leave the site in a clean and safe condition;

(b) terminate all subcontracts, except those to be assigned to the Purchaser pursuant to Clause 41.3.3 (d) (ii);

(c) remove all Supplier's Equipment from the site and repatriate the Supplier's and its Subcontractor's personnel from the site.

(d) In addition, the Supplier, subject to the payment specified in GCC Clause 41.3.4, shall:

(i) deliver to the Purchaser the parts of the System executed by the Supplier up to the date of termination;

(ii) to the extent legally possible, assign to the Purchaser all right, title, and benefit of the Supplier to the System, or Subsystems, as of the date of termination, and, as may be required by the Purchaser, in any subcontracts concluded between the Supplier and its Subcontractors;

(iii) to the extent legally possible, deliver to the Purchaser all drawings, specifications, and other documents prepared by the Supplier or its Subcontractors as of the date of termination in connection with the System.

41.3.4 If the Contract is terminated under GCC Clauses 41.3.1 or 41.3.2, the Purchaser shall pay to the Supplier all payments specified in GCC Clause 41.1.3 and reasonable compensation for all loss, except for loss of profit, or damage sustained by the Supplier arising out of, in connection with, or in consequence of such termination.

41.3.5 Termination by the Supplier pursuant to this GCC Clause 41.3 is without prejudice to any other rights

or remedies of the Supplier that may be exercised in lieu of or in addition to rights conferred by GCC Clause 41.3.

41.4 In this GCC Clause 41, the expression "portion of the System executed" shall include all work executed, Services provided, and all Information Technologies, or other Goods acquired (or subject to a legally binding obligation to purchase) by the Supplier and used or intended to be used for the purpose of the System, up to and including the date of termination.

41.5 In this GCC Clause 41, in calculating any monies due from the Purchaser to the Supplier, account shall be taken of any sum previously paid by the Purchaser to the Supplier under the Contract, including any advance payment paid **pursuant to the SCC.**

42. Assignment

42.l Neither the Purchaser nor the Supplier shall, without the express prior written consent of the other, assign to any third party the Contract or any part thereof, or any right, benefit, obligation, or interest therein or thereunder, except that the Supplier shall be entitled to assign either absolutely or by way of charge any monies due and payable to it or that may become due and payable to it under the Contract.

I. SETTLEMENT OF DISPUTES

43. Settlement of Disputes

43.1 Adjudication

43.1.1 If any dispute of any kind whatsoever shall arise between the Purchaser and the Supplier in connection with or arising out of the Contract, including without prejudice to the generality of the foregoing, any question regarding its existence, validity, or termination, or the operation of the System (whether during the progress of implementation or after its achieving Operational Acceptance and whether before or after the termination, abandonment, or breach of the Contract), the parties shall seek to resolve any such dispute by mutual consultation. If the parties fail to resolve such a dispute by mutual consultation within fourteen (14) days after one party has notified the other in writing of the dispute, then, if the Contract Agreement in Appendix 2 includes and

names an Adjudicator, the dispute shall, within another fourteen (14) days, be referred in writing by either party to the Adjudicator, with a copy to the other party. If there is no Adjudicator specified in the Contract Agreement, the mutual consultation period stated above shall last twenty-eight (28) days (instead of fourteen), upon expiry of which either party may move to the notification of arbitration pursuant to GCC Clause 6.2.1.

43.1.2 The Adjudicator shall give his or her decision in writing to both parties within twenty-eight (28) days of the dispute being referred to the Adjudicator. If the Adjudicator has done so, and no notice of intention to commence arbitration has been given by either the Purchaser or the Supplier within fifty-six (56) days of such reference, the decision shall become final and binding upon the Purchaser and the Supplier. Any decision that has become final and binding shall be implemented by the parties forthwith.

43.1.3 The Adjudicator shall be paid an hourly fee at the rate specified in the Contract Agreement plus reasonable expenditures incurred in the execution of duties as Adjudicator, and these costs shall be divided equally between the Purchaser and the Supplier.

43.1.4 Should the Adjudicator resign or die, or should the Purchaser and the Supplier agree that the Adjudicator is not fulfilling his or her functions in accordance with the provisions of the Contract, a new Adjudicator shall be jointly appointed by the Purchaser and the Supplier. Failing agreement between the two within twenty-eight (28) days, the new Adjudicator shall be appointed at the request of either party by the Appointing Authority **specified in the SCC,** or, if no Appointing Authority is **specified in SCC,** the Contract shall, from this point onward and until the parties may otherwise agree on an Adjudicator or an Appointing Authority, be implemented as if there is no Adjudicator.

43.2 Arbitration

43.2.1 If

(a) the Purchaser or the Supplier is dissatisfied with the Adjudicator's decision and acts before this

decision has become final and binding pursuant to GCC Clause 43.1.2, or

(b) the Adjudicator fails to give a decision within the allotted time from referral of the dispute pursuant to GCC Clause 43.1.2, and the Purchaser or the Supplier acts within the following fourteen (14) days, or

(c) in the absence of an Adjudicator from the Contract Agreement, the mutual consultation pursuant to GCC Clause 43.1.1 expires without resolution of the dispute and the Purchaser or the Supplier acts within the following fourteen (14) days,

then either the Purchaser or the Supplier may act to give notice to the other party, with a copy for information to the Adjudicator in case an Adjudicator had been involved, of its intention to commence arbitration, as provided below, as to the matter in dispute, and no arbitration in respect of this matter may be commenced unless such notice is given.

43.2.2 Any dispute in respect of which a notice of intention to commence arbitration has been given, in accordance with GCC Clause 43.2.1, shall be finally settled by arbitration. Arbitration may be commenced prior to or after Installation of the Information System.

43.2.3 Arbitration proceedings shall be conducted in accordance with the rules of procedure **specified in the SCC.**

43.3 Notwithstanding any reference to the Adjudicator or arbitration in this clause,

(a) the parties shall continue to perform their respective obligations under the Contract unless they otherwise agree;

(b) the Purchaser shall pay the Supplier any monies due the Supplier.

APPENDIX I

Fraud and Corruption

(Text in this Appendix shall not be modified)

1. Purpose

1.1 The Bank's Anti-Corruption Guidelines and this annex apply with respect to procurement under Bank Investment Project Financing operations.

2. Requirements

2.1 The Bank requires that Borrowers (including beneficiaries of Bank financing); bidders, consultants, contractors and suppliers; any sub-contractors, sub-consultants, service providers or suppliers; any agents (whether declared or not); and any of their personnel, observe the highest standard of ethics during the procurement process, selection and contract execution of Bank-financed contracts, and refrain from Fraud and Corruption.

2.2 To this end, the Bank:

a. Defines, for the purposes of this provision, the terms set forth below as follows:

i. "corrupt practice" is the offering, giving, receiving, or soliciting, directly or indirectly, of anything of value to influence improperly the actions of another party;

ii. "fraudulent practice" is any act or omission, including misrepresentation, that knowingly or recklessly misleads, or attempts to mislead, a party to obtain financial or other benefit or to avoid an obligation;

iii. "collusive practice" is an arrangement between two or more parties designed to achieve an improper purpose, including to influence improperly the actions of another party;

iv. "coercive practice" is impairing or harming, or threatening to impair or harm, directly or indirectly, any party or the property of the party to influence improperly the actions of a party;

v. "obstructive practice" is:

(a) deliberately destroying, falsifying, altering, or concealing of evidence material to the investigation or making false statements to investigators in order to materially impede a Bank investigation into allegations of a corrupt, fraudulent, coercive, or collusive practice; and/or threatening, harassing, or intimidating any party to prevent it from disclosing its knowledge of matters relevant to the investigation or from pursuing the investigation; or

(b) acts intended to materially impede the exercise of the Bank's inspection and audit rights provided for under paragraph 2.2 e. below.

b. Rejects a proposal for award if the Bank determines that the firm or individual recommended for award, any of its personnel, or its agents, or its sub-consultants, sub-

contractors, service providers, suppliers and/ or their employees, has, directly or indirectly, engaged in corrupt, fraudulent, collusive, coercive, or obstructive practices in competing for the contract in question;

c. In addition to the legal remedies set out in the relevant Legal Agreement, may take other appropriate actions, including declaring misprocurement, if the Bank determines at any time that representatives of the Borrower or of a recipient of any part of the proceeds of the loan engaged in corrupt, fraudulent, collusive, coercive, or obstructive practices during the procurement process, selection and/or execution of the contract in question, without the Borrower having taken timely and appropriate action satisfactory to the Bank to address such practices when they occur, including by failing to inform the Bank in a timely manner at the time they knew of the practices;

d. Pursuant to the Bank's Anti-Corruption Guidelines, and in accordance with the Bank's prevailing sanctions policies and procedures, may sanction a firm or individual, either indefinitely or for a stated period of time, including by publicly declaring such firm or individual ineligible (i) to be awarded or otherwise benefit from a Bank-financed contract, financially or in any other manner;[1] (ii) to be a nominated[2] sub-contractor, consultant, manufacturer or supplier, or service provider of an otherwise eligible firm being awarded a Bank-financed contract; and (iii) to receive the proceeds of any loan made by the Bank or otherwise to participate further in the preparation or implementation of any Bank-financed project;

e. Requires that a clause be included in bidding/request for proposals documents and in contracts financed by a Bank loan, requiring (i) bidders, consultants, contractors, and suppliers, and their sub-contractors, sub-consultants, service providers, suppliers, agents personnel, permit the Bank to inspect[3] all accounts, records and other documents relating to the submission of bids and contract performance, and to have them audited by auditors appointed by the Bank.

---

1 For the avoidance of doubt, a sanctioned party's ineligibility to be awarded a contract shall include, without limitation, (i) applying for pre-qualification, expressing interest in a consultancy, and bidding, either directly or as a nominated sub-contractor, nominated consultant, nominated manufacturer or supplier, or nominated service provider, in respect of such contract, and (ii) entering into an addendum or amendment introducing a material modification to any existing contract.

2 A nominated sub-contractor, nominated consultant, nominated manufacturer or supplier, or nominated service provider (different names are used depending on the particular bidding document) is one which has been: (i) included by the bidder in its pre-qualification application or bid because it brings specific and critical experience and know-how that allow the bidder to meet the qualification requirements for the particular bid; or (ii) appointed by the Borrower.

3 Inspections in this context usually are investigative (i.e., forensic) in nature. They involve fact-finding activities undertaken by the Bank or persons appointed by the Bank to address specific matters related to investigations/audits, such as evaluating the veracity of an allegation of possible Fraud and Corruption, through the appropriate mechanisms. Such activity includes but is not limited to: accessing and examining a firm's or individual's financial records and information, and making copies thereof as relevant; accessing and examining any other documents, data and information (whether in hard copy or electronic format) deemed relevant for the investigation/audit, and making copies thereof as relevant; interviewing staff and other relevant individuals; performing physical inspections and site visits; and obtaining third party verification of information.

SECTION IX - SPECIAL CONDITIONS OF CONTRACT
Table of Clauses

Special Conditions of Contract

The following Special Conditions of Contract (SCC) shall supplement or amend the General Conditions of Contract (GCC). Whenever there is a conflict, the provisions of the SCC shall prevail over those in the General Conditions of Contract. For the purposes of clarity, any referenced GCC clause numbers are indicated in the left column of the SCC.

A. CONTRACT AND INTERPRETATION

1. Definitions (GCC Clause 1)

GCC 1.1 (a) (ix)	The applicable edition of the Procurement Regulation is dated: July, 2016.
GCC 1.1 (b) (i)	The Purchaser is: Bangladesh Computer Council (BCC) represented by the Project Director**,** Leveraging ICT for Growth, Employment and Governance Project**.**
GCC 1.1 (b) (ii)	The Project Manager is: **Project Director,** Leveraging ICT for Growth, Employment and Governance Project Bangladesh Computer Council (BCC), ICT Tower (2nd Floor), Plot # E-14/X, Agargaon, Sher-e-Bangla Nagar, Dhaka – 1207, Bangladesh. Telephone: +880-2-8181381; Fax: +880-2-818138 E-mail: pd.lict@bcc.net.bd
GCC 1.1 (e) (i)	The Purchaser's Country is: **Bangladesh**.
GCC 1.1 (e) (x)	**There are no Special Conditions associated with GCC 1.1 (e) (x).** The Contract shall continue in force until the Information System and all the Services have been provided **up to 3 years (warranty period) plus installation period from the commencement date of contract** unless the Contract is terminated earlier in accordance with the terms set out in the Contract.
GCC 1.1 (e) (xiii)	The Post-Warranty Services Period is **None** starting with the completion of the Warranty Period.

2. Notices (GCC Clause 4)

GCC 4.3	Address of the Project Manager: **Project Director,** Leveraging ICT for Growth, Employment and Governance Project Bangladesh Computer Council (BCC), ICT Tower (2nd Floor),

	Plot # E-14/X, Agargaon, Sher-e-Bangla Nagar, Dhaka – 1207, Bangladesh. Telephone: +880-2-8181381; Fax: +880-2-818138 E-mail: pd.lict@bcc.net.bd Fallback address of the Purchaser: As above.

3. Governing Law (GCC Clause 5)

GCC 5.1	The Contract shall be interpreted in accordance with the laws of: **Bangladesh**

B. SUBJECT MATTER OF CONTRACT

4. Scope of the System (GCC Clause 7)

GCC 7.3	The Supplier's obligations under the Contract will include the following recurrent cost items, as identified in the Recurrent Cost tables in the Supplier's Bid: **Not Applicable.**

5. Time for Commencement and Operational Acceptance (GCC Clause 8)

GCC 8.1	The Supplier shall commence work on the System within: **10** [*ten]* days from the Effective Date of the Contract.

6. Supplier's Responsibilities (GCC Clause 9)

GCC 9.9	The following sustainable procurement contractual provisions apply: (i) The supplier shall use efficient technologies to reduce the amount of energy spent; (ii) The supplier shall work to remove redundant data, minimize and consolidate the number of redundant databases and eliminate outdated and unused systems and servers.

C. PAYMENT

7. Contract Price (GCC Clause 11)

GCC 11.2 (b)	Adjustments to the Contract Price shall be as follows*:* **Not applicable.**

8. Terms of Payment (GCC Clause 12)

GCC 12.1	Subject to the provisions of GCC Clause 12 (Terms of Payment), the Purchaser shall pay the Contract Price to the Supplier according to the categories and in the manner specified below. Only the categories Advance Payment and Complete System Integration relate to the entire Contract Price. In other payment categories, the term "total Contract Price" means the total cost of goods or services under the specific payment category. Within each such category, the Contract Implementation Schedule may trigger pro-rata payments for the portion of the total Contract Price for the category corresponding to the goods or services actually Delivered, Installed, or Operationally Accepted, at unit prices and in the currencies specified in the Price Schedules of the Contract Agreement. (a) **Advance Payment:** Ten percent (10%) of the entire Contract Price will be paid against receipt of a claim accompanied by the Advance Payment Security specified in GCC Clause 13.2. (b) **Stage 1: Design**: Ten percent (10%) of the total Contract Price will be paid upon receipt of invoice claim supported by the 'acceptance certificate'. (c) **Stage 2 : Technology delivery**: **On Delivery:** 40% (forty percent) of the total Contract Price will be paid after shipment through irrevocable confirmed letter of credit (LC), upon submission of documents specified in GCC Clause 22.5 and associated SCC. (d) **Stage 3 : Commissioning (installing)**: **On Acceptance:** 30% (thirty percent) of the total Contract Price will be paid upon receipt of invoice claim supported by the certificate of User Acceptance Test (UAT), issued by the Purchaser following successful completion of Operational, Interoperability and Integration Tests for all items supplied, installed, configured and deployed in the Cyber Defense Training Center. User Acceptance Test (UAT) includes the above-mentioned tests: (e) Complete System Integration ten percent (10%) of the entire Contract Price, exclusive of all Recurrent Costs, as final payment against Operational

	Acceptance of the System as an integrated whole. If advance payment is not taken by the bidder, the amount will be paid with the **Complete System Integration** after successful completion of the operational acceptance tests and Complete System Integration.
GCC 12.3	The Purchaser shall pay to the Supplier interest on the delayed payments at a rate of: On foreign currency: London Inter Bank Offered Rate (LIBOR)+ 1% On local currency : Dhaka Inter Bank Offered Rate (DIBOR) The payment delay period after which the Purchaser shall pay interest to the supplier shall be 45 days after submission of an invoice or request for payment by the supplier, and after the Purchaser has accepted it.
GCC 12.4	For Goods and Services supplied locally, the Purchaser will pay the Supplier in **Bangladesh Taka**.
GCC 12.5	Payment for Goods supplied from outside the Purchaser's Country shall be in the form of: **an irrevocable letter of credit.**

9. Securities (GCC Clause 13)

GCC 13.3.1	The Performance Security shall be denominated in **the major currency of the Contract** for an amount equal to **ten (10)** percent of the Contract Price, excluding any Recurrent Costs.
GCC 13.3.4	During the Warranty Period (i.e., after Operational Acceptance of the System), the Performance Security shall be reduced to **five (5)** percent of the Contract Price, excluding any Recurrent Costs.

10. Taxes and Duties (GCC Clause 14)

GCC 14.1	In addition to Clause 14.1 following shall be added: Customs Duties and Value Added Taxes (CD &VAT) of the goods to be imported under the Contract, incurred at the port of entry of the Purchaser's Country, and payment to clearing and forwarding (C&F) agent shall be initially paid by the S**upplier, and the Purchaser shall reimburse the same, within 30 days, against production of supporting documents by the Supplier**. This Customs Duty, VAT clearing and forwarding (C&F) agent cost shall not be included in the total Contract Price. The Purchaser shall deduct Value Added Tax (VAT) and Income Tax

	(IT) at source at the rate applicable in accordance with the prevailing provision of Bangladesh-National Board of Revenue, at the time of making any payment to the Supplier. Pursuant to this provision, the Purchaser shall deduct VAT and IT at source and deposit the same to the government's exchequer and provide the records of such deposits to the supplier for facilitating its Tax assessment or obligations in Bangladesh.

D. INTELLECTUAL PROPERTY

11. Copyright (GCC Clause 15)

GCC 15.3	The Purchaser may assign, license, or otherwise voluntarily transfer its contractual rights to use the Standard Software or elements of the Standard Software, without the Supplier's prior written consent, under the following circumstances: **In case of reorganization of the responsibility to any successor organization.**
GCC 15.4	The Purchaser's and Supplier's rights and obligations with respect to Custom Software or elements of the Custom Software are as follows : **"not applicable"** The Purchaser's and Supplier's rights and obligations with respect to Custom Materials or elements of the Custom Materials are as follows : **"not applicable"**
GCC 15.5	***There are no Special Conditions of Contract applicable to GCC Clause 15.5.***

12. Software License Agreements (GCC Clause 16)

GCC 16.1 (a) (iii)	The Standard Software license shall be valid **throughout the territory of Bangladesh.** **The supplied software licenses shall be registered through Regional Headquarters, under which Bangladesh falls, of the global software vendors for ensuring convenient upgrade facility and renewal (as and when necessary).**
GCC 16.1 (a) (iv)	***There are no Special Conditions of Contract applicable to GCC Clause 16.1 (a) (iv).***

GCC 16.1 (b) (vi)	The Software license shall permit the Software to be disclosed to and reproduced for use (including a valid sublicense) by **support service suppliers or their subcontractors, exclusively for such suppliers or subcontractors in the performance of their support service contracts**, subject to the same restrictions set forth in this Contract.
GCC 16.1 (b) (vii)	In addition to the persons specified in GCC Clause 16.1 (b) (vi), the Software may be disclosed to, and reproduced for use by **the Purchaser's authorized staff** subject to the same restrictions as are set forth in this Contract.
GCC 16.2	***There are no Special Conditions of Contract applicable to GCC Clause 16.2***

13. Confidential Information (GCC Clause 17)

GCC 17.1	***There are no Special Conditions of Contract applicable to GCC Clause 17.1***

E. SUPPLY, INSTALLATION, TESTING, COMMISSIONING, AND ACCEPTANCE OF THE SYSTEM

14. Representatives (GCC Clause 18)

GCC 18.1	The Purchaser's Project Manager shall have the following additional powers and / or limitations to his or her authority to represent the Purchaser in matters relating to the Contract **No additional powers or limitations.**
GCC 18.2.2	The Supplier's Representative shall have the following additional powers and / or limitations to his or her authority to represent the Supplier in matters relating to the Contract **No additional powers or limitations.**

15. Project Plan (GCC Clause 19)

GCC 19.1	Chapters in the Project Plan shall address the following subject**:** ***(a) Project Organization and Management Sub-Plan, including management authorities, responsibilities, and contacts, as well as task, time and resource-bound schedules (in GANTT format);***

	(b) Methodology ***(c) Implementation Sub-Plan;*** ***(d) Training Sub-Plan;*** ***(e) Testing and Quality Assurance Sub-Plan;*** ***(f) Warranty Defect Repair and Technical Support Service Sub-Plan*** Further details regarding the required contents of each of the above chapters are contained in the Technical Requirements, **Section VII.**
GCC 19.6	***The Supplier shall submit to the Purchaser:*** ***(i) monthly inspection and quality assurance reports*** ***(ii) monthly training participants test results*** ***(iii) monthly log of service calls and problem resolutions***

16. Subcontracting (GCC Clause 20)

GCC 20	**Sub-contracting shall be allowed.** Bidder may subcontract refurbishment/construction works - however, the aggregated sub-contracting shall not be more than 20% of the total contract price**.**

17. Design and Engineering (GCC Clause 21)

GCC 21.3.1	*The Supplier shall prepare and furnish to the Project Manager the following documents for which the Supplier must obtain the Project Manager's approval before proceeding with work on the System or any Subsystem covered by the documents:* ***a) detailed site surveys;*** ***b) final Subsystem configurations.***
GCC 22.5	**The Supplier shall provide the Purchaser with shipping and other documents as follows;** (a) Original plus five (05) copies of Bill of Lading (b) Original plus five (05) copies of Supplier's invoice showing goods' description, quantity, unit price, total amount; (c) Original plus five (05) copies of the packing list identifying the contents of each package (d) Original plus five (05) copies of manufacturer's warranty certificate

	(e) Original plus five (05) copies the manufacturer's/Supplier's factory inspection report (f) Original plus five (05) copies of the inspection certificate(s) issued by the nominated inspection agency (or the Purchaser) (if applicable); (g) Original plus five (05) copies of certificate of origin. *The above documents shall be received by the Purchaser at least two weeks before arrival of the Goods at the place of arrival and, if not received, the Supplier will be responsible for any consequent expenses.* 2. For Goods supplied from within Bangladesh, upon delivery of the Goods to the transporter, the Supplier shall notify the purchaser and mail the following documents to the purchaser: a) One original plus five copies of the Supplier's invoice showing Goods' description, quantity, unit price, and total amount; b) Delivery note, railway receipt, or truck receipt; c) Manufacturer's or Supplier's warranty certificate; d) Inspection certificate issued by the nominated inspection agency, and the Supplier's factory inspection report; and e) Certificate of country of origin issued by the Chamber of Commerce or equivalent authority in the country of origin in duplicate. *The above documents shall be received by the purchaser before arrival of the Goods and, if not received, the Supplier will be responsible for any consequent expenses.*

18. Product Upgrades (GCC Clause 23)

GCC 23.4	The Supplier shall provide the Purchaser **with all new versions, releases, and updates to all Standard Software during the Contract Period, for free, as specified in the GCC.**

19. Inspections and Tests (GCC Clause 25)

GCC 25	***There are no Special Conditions of Contract applicable to GCC Clause 25.***

20. Commissioning and Operational Acceptance (GCC Clause 27)

GCC 27.2.1	Operational Acceptance Testing shall be conducted in accordance with **Section VII Technical Requirements where acceptance testing details are given.**
GCC 27.2.2	If the Operational Acceptance Test of the System, or Subsystem(s), cannot be successfully completed within **no more than fourteen (14)** days from the date of Installation or any other period agreed upon by the Purchaser and the Supplier, then GCC Clause 27.3.5 (a) or (b) shall apply, as the circumstances may dictate.

F. GUARANTEES AND LIABILITIES

21. Operational Acceptance Time Guarantee (GCC Clause 28)

GCC 28.2	Liquidated damages shall be assessed at **one half of one percent (0.5%) per week. This will be applicable on each stage of payment milestones as mentioned in the SCC Clause corresponding to GCC 12.1 (Payment Schedule).** The maximum liquidated damages are **ten percent (10%) o**f the Contract Price, or relevant part of the Contract Price if the liquidated damages apply to a Subsystem.
GCC 28.3	Liquidated damages shall be assessed *o***nly with respect to achieving Operational Acceptance of each 'stage' of payment milestone as mentioned in the SCC Clause corresponding to GCC 12.1 (Payment Schedule).**

22. Defect Liability (GCC Clause 29)

GCC 29.1	***There are no Special Conditions of Contract applicable to GCC Clause 29.1.***
GCC 29.4	**The Warranty Period of Thirty-Six (36) months shall begin from the date of Operational Acceptance of the System or Subsystem and extend for the periods that may apply to software products.**
GCC 29.10	During the Warranty Period, the Supplier must commence the work necessary

	to remedy defects or damage within the time as indicated **the Technical Specifications in particular Sections and in Service Levels.**

23. Functional Guarantees (GCC Clause 30)

GCC 30	***There are no Special Conditions of Contract applicable to GCC Clause 30.***

G. RISK DISTRIBUTION

24. Insurances (GCC Clause 37)

GCC 37.1 (c)	The Supplier shall obtain Third-Party Liability Insurance in accordance with the statutory requirements of Bangladesh. The insured Parties shall be ***the Supplier and the Purchaser*** The Insurance shall cover the period from ***beginning date, relative to the Effective Date of the Contract*** *until* ***expiration date, relative to the Effective Date of the Contract or its completion.***
GC 37.1 (e)	The Supplier shall obtain Worker's Compensation Insurance in accordance with the statutory requirements of **Banglades*h***. Specifically the Insurance shall cover the period from *beginning* **date, relative to the Effective Date of the Contract** until **expiration date, relative to the Effective Date of the Contract or its completion**. The Supplier shall obtain Employer's Liability Insurance in accordance with the statutory requirements of **Bangladesh.** Specifically: the Insurance shall cover the period from ***beginning date, relative to the Effective Date of the Contract*** *until* ***expiration date, relative to the Effective Date of Contract or its completion.***

H. CHANGE IN CONTRACT ELEMENTS

25. Changes to the System (GCC Clause 39)

GCC 39.4	**Value Engineering: Not Applicable.**

I. SETTLEMENT OF DISPUTES

26. Settlement of Disputes (GCC Clause 43)

GCC 43.1.4	The Appointing Authority for the Adjudicator is: (a) if the Supplier is foreign (including a Joint Venture when at least one partner is foreign): **International Chamber of Commerce.** (b) if the Supplier is a national of the Purchaser's country **President of the Institution of Engineers, Bangladesh (IEB).**
GCC 43.2.3	*If the Supplier is foreign (including a Joint Venture when at least one partner is foreign), the Contract shall contain the following provision:* Arbitration proceedings shall be conducted in accordance with the rules of arbitration of*:* **UNCITRAL**. These rules, in the version in force at the time of the request for arbitration, will be deemed to form part of this Contract. *If the Supplier is a national of the Purchaser's country, the Contract shall contain the following provision:* Any dispute between the Purchaser and a Supplier arising in connection with the present Contract shall be referred to arbitration in accordance with the laws of the Purchaser's country.

SECTION X - CONTRACT FORMS

Notes to the Purchaser on preparing the Contract Forms

Performance Security: Pursuant to GCC Clause 13.3, the successful Bidder is required to provide the Performance Security within twenty-eight (28) days of notification of Contract award.

Advance Payment Security: Pursuant to Clause 13.2, the successful Bidder is required to provide a bank guarantee securing the Advance Payment, if the SCC related to GCC Clause 12.1 provides for an Advance Payment.

Installation and Operational Acceptance Certificates: Recommended formats for these certificates are included in this SPD. Unless the Purchaser has good reason to require procedures that differ from those recommended, or to require different wording in the certificates, the procedures and forms shall be included unchanged. If the Purchaser wishes to amend the recommended procedures and/or certificates, it may propose alternatives for the approval of the World Bank before release of the bidding document to potential Bidders.

Change Order Procedures and Forms: Similar to the Installation and Operational Acceptance Certificates, the Change Estimate Proposal, Estimate Acceptance, Change Proposal, Change Order, and related Forms should be included in the bidding document unaltered. If the Purchaser wishes to amend the recommended procedures and/or certificates, it may propose alternatives for the approval of the World Bank before release of the bidding document.

Notes to Bidders on working with the Sample Contractual Forms

The following forms are to be completed and submitted by the successful Bidder following notification of award: (i) Contract Agreement, with all Appendices; (ii) Performance Security; and (iii) Advance Payment Security.

- Contract Agreement: In addition to specifying the parties and the Contract Price, the Contract Agreement is where the: (i) Supplier Representative; (ii) if applicable, agreed Adjudicator and his/her compensation; and (iii) the List of Approved Subcontractors are specified. In addition, modifications to the successful Bidder's Bid Price Schedules are attached to the Agreement. These contain corrections and adjustments to the Supplier's bid prices to correct errors, adjust the Contract Price to reflect – if applicable - any extensions to bid validity beyond the last day of original bid validity plus 56 days, etc.
- Performance Security: Pursuant to GCC Clause 13.3, the successful Bidder is required to provide the Performance Security in the form contained in this section of these bidding documents and in the amount specified in accordance with the SCC.
- Advance Payment Security: Pursuant to GCC Clause 13.2, the successful Bidder is required to provide a bank guarantee for the full amount of the Advance Payment - if an Advance Payment is specified in the SCC for GCC Clause 12.1 -

in the form contained in this section of these bidding documents or another form acceptable to the Purchaser. If a Bidder wishes to propose a different Advance Payment Security form, it should submit a copy to the Purchaser promptly for review and confirmation of acceptability before the bid submission deadline.

The Purchaser and Supplier will use the following additional forms during Contract implementation to formalize or certify important Contract events: (i) the Installation and Operational Acceptance Certificates; and (ii) the various Change Order forms. These and the procedures for their use during performance of the Contract are included in the bidding documents for the information of Bidders.

1. CONTRACT AGREEMENT

THIS CONTRACT AGREEMENT is made

the ***[insert: ordinal]*** day of ***[insert: month], [insert: year].***

BETWEEN

(1) ***[insert: Name of Purchaser],*** a ***[insert: description of type of legal entity, for example, an agency of the Ministry of . . .]*** of the Government of ***[insert: country of Purchaser],*** or corporation incorporated under the laws of ***[insert: country of Purchaser]*** and having its principal place of business at ***[insert: address of Purchaser]*** (hereinafter called "the Purchaser"), and

(2) ***[insert: name of Supplier],*** a corporation incorporated under the laws of ***[insert: country of Supplier]*** and having its principal place of business at ***[insert: address of Supplier]*** (hereinafter called "the Supplier").

WHEREAS the Purchaser desires to engage the Supplier to supply, install, achieve Operational Acceptance of, and support the following Information System ***[insert: brief description of the Information System]*** ("the System"), and the Supplier has agreed to such engagement upon and subject to the terms and conditions appearing below in this Contract Agreement.

NOW IT IS HEREBY AGREED as follows:

Article 1. Contract Documents

1.1 Contract Documents (Reference GCC Clause 1.1 (a) (ii))

The following documents shall constitute the Contract between the Purchaser and the Supplier, and each shall be read and construed as an integral part of the Contract:

(a) This Contract Agreement and the Appendices attached to the Contract Agreement

(b) Special Conditions of Contract

(c) General Conditions of Contract

(d) Technical Requirements (including Implementation Schedule)

(e) The Supplier's bid and original Price Schedules

(f) ***[Add here: any other documents]***

1.2 Order of Precedence (Reference GCC Clause 2)

In the event of any ambiguity or conflict between the Contract

Documents listed above, the order of precedence shall be the order in which the Contract Documents are listed in Article 1.1 (Contract Documents) above, provided that Appendix 7 shall prevail over all provisions of the Contract Agreement and the other Appendices attached to the Contract Agreement and all the other Contract Documents listed in Article 1.1 above.

1.3 Definitions (Reference GCC Clause 1)

Capitalized words and phrases used in this Contract Agreement shall have the same meanings as are ascribed to them in the General Conditions of Contract.

Article 2.

Contract Price and Terms of Payment

2.1 Contract Price (Reference GCC Clause 1.1(a)(viii) and GCC Clause 11)

The Purchaser hereby agrees to pay to the Supplier the Contract Price in consideration of the performance by the Supplier of its obligations under the Contract. The Contract Price shall be the aggregate of: ***[insert: amount of foreign currency A in words], [insert: amount in figures],*** plus ***[insert: amount of foreign currency B in words], [insert: amount in figures],*** plus ***[insert: amount of foreign currency C in words], [insert: amount in figures], [insert: amount of local currency in words], [insert: amount in figures],*** as specified in the Grand Summary Price Schedule.

The Contract Price shall be understood to reflect the terms and conditions used in the specification of prices in the detailed price schedules, including the terms and conditions of the associated Incoterms, and the taxes, duties and related levies if and as identified.

Article 3.

Effective Date for Determining Time for Operational Acceptance

3.1 Effective Date (Reference GCC Clause 1.1 (e) (ix))

The time allowed for supply, installation, and achieving Operational Acceptance of the System shall be determined from the date when all of the following conditions have been fulfilled:

(a) This Contract Agreement has been duly executed for and on behalf of the Purchaser and the Supplier;

(b) The Supplier has submitted to the Purchaser the performance security and the advance payment security, in accordance with GCC Clause 13.2 and GCC Clause 13.3;

(c) The Purchaser has paid the Supplier the advance payment, in accordance with GCC Clause 12;

Each party shall use its best efforts to fulfill the above conditions for which it is responsible as soon as practicable.

3.2 If the conditions listed under 3.1 are not fulfilled within two (2)

months from the date of this Contract Agreement because of reasons not attributable to the Supplier, the parties shall discuss and agree on an equitable adjustment to the Contract Price and the Time for Achieving Operational Acceptance and/or other relevant conditions of the Contract.

Article 4. Appendixes

4.1 The Appendixes listed below shall be deemed to form an integral part of this Contract Agreement.

4.2 Reference in the Contract to any Appendix shall mean the Appendixes listed below and attached to this Contract Agreement, and the Contract shall be read and construed accordingly.

APPENDIXES

Appendix 1. Supplier's Representative
Appendix 2. Adjudicator *[if there is no Adjudicator, state **"not applicable"**]*
Appendix 3. List of Approved Subcontractors
Appendix 4. Categories of Software
Appendix 5. Custom Materials
Appendix 6. Revised Price Schedules (if any)
Appendix 7. Minutes of Contract Finalization Discussions and Agreed-to Contract Amendments

IN WITNESS WHEREOF the Purchaser and the Supplier have caused this Agreement to be duly executed by their duly authorized representatives the day and year first above written.

For and on behalf of the Purchaser

Signed:

in the capacity of ***[insert: title or other appropriate designation]***

in the presence of

For and on behalf of the Supplier

Signed:

in the capacity of ***[insert: title or other appropriate designation]***

in the presence of

CONTRACT AGREEMENT

dated the ***[insert: number]*** day of ***[insert: month], [insert: year]***

BETWEEN

[insert: name of Purchaser], "the Purchaser"

and

[insert: name of Supplier], "the Supplier"

Appendix 1. Supplier's Representative

In accordance with GCC Clause 1.1 (b) (iv), the Supplier's Representative is:

Name: ***[insert: name and provide title and address further below, or state "to be nominated within fourteen (14) days of the Effective Date"]***

Title: ***[if appropriate, insert: title]***

In accordance with GCC Clause 4.3, the Supplier's addresses for notices under the Contract are:

Address of the Supplier's Representative: ***[as appropriate, insert: personal delivery, postal, cable, telegraph, telex, facsimile, electronic mail, and/or EDI addresses.]***

Fallback address of the Supplier: ***[as appropriate, insert: personal delivery, postal, cable, telegraph, telex, facsimile, electronic mail, and/or EDI addresses.]***

Appendix 2. Adjudicator

In accordance with GCC Clause 1.1 (b) (vi), the agreed-upon Adjudicator is:

Name: ***[insert: name]***

Title: ***[insert: title]***

Address: ***[insert: postal address]***

Telephone: ***[insert: telephone]***

In accordance with GCC Clause 6.1.3, the agreed-upon fees and reimbursable expenses are:

Hourly Fees: ***[insert: hourly fees]***

Reimbursable Expenses: ***[list: reimbursables]***

Pursuant to GCC Clause 6.1.4, if at the time of Contract signing, agreement has not been reached between the Purchaser and the Supplier, an Adjudicator will be appointed by the Appointing Authority named in the SCC.

Appendix 3. List of Approved Subcontractors

The Purchaser has approved use of the following Subcontractors nominated by the Supplier for carrying out the item or component of the System indicated. Where more than one Subcontractor is listed, the Supplier is free to choose between them, but it must notify the Purchaser of its choice sufficiently in advance of the time when the subcontracted work needs to commence to give the Purchaser reasonable time for review. In accordance with GCC Clause 20.1, the Supplier is free to submit proposals for Subcontractors for additional items from time to time. No subcontracts shall be placed with any such Subcontractors for additional items until the Subcontractors have been approved in writing by the Purchaser and their names have been added to this list of Approved Subcontractors, subject to GCC Clause 20.3.

[specify: item, approved Subcontractors, and their place of registration that the Supplier proposed in the corresponding attachment to its bid and that the Purchaser approves that the Supplier engage during the performance of the Contract. Add additional pages as necessary.]

Item	Approved Subcontractors	Place of Registration

Appendix 4. Categories of Software

The following table assigns each item of Software supplied and installed under the Contract to one of the three categories: (i) System Software, (ii) General-Purpose Software, or (iii) Application Software; and to one of the two categories: (i) Standard Software or (ii) Custom Software.

	(select one per item)			(select one per item)	
Software Item	System Software	General-Purpose Software	Application Software	Standard Software	Custom Software

Appendix 5. Custom Materials

The follow table specifies the Custom Materials the Supplier will provide under the Contract.

Custom Materials

Appendix 6. Revised Price Schedules

The attached Revised Price Schedules (if any) shall form part of this Contract Agreement and, where differences exist, shall supersede the Price Schedules contained in the Supplier's Bid. These Revised Price Schedules reflect any corrections or adjustments to the Supplier's bid price, pursuant to the ITB Clauses 30.3 and 38.2.

Appendix 7. Minutes of Contract Finalization Discussions and Agreed-to Contract Amendments

The attached Contract amendments (if any) shall form part of this Contract Agreement and, where differences exist, shall supersede the relevant clauses in the GCC, SCC, Technical Requirements, or other parts of this Contract as defined in GCC Clause 1.1 (a) (ii).

2. PERFORMANCE AND ADVANCE PAYMENT SECURITY FORMS

Performance Security Form (Bank Guarantee)

(Bank Guarantee)

[The bank, as requested by the successful Bidder, shall fill in this form in accordance with the instructions indicated]

[Guarantor letterhead or SWIFT identifier code]

_____

*[insert: **Bank's Name, and Address of Issuing Branch or Office**]*

Beneficiary: *[insert: **Name and Address of Purchaser**]*

Date: *[insert: **date**]*

PERFORMANCE GUARANTEE No.: *[insert: **Performance Guarantee Number**]*

Guarantor: *[Insert name and address of place of issue, unless indicated in the letterhead*

We have been informed that on *[insert: **date of award**]* you awarded Contract No. *[insert: **Contract number**]* for *[insert: **title and/or brief description of the Contract**]* (hereinafter called "the Contract") to *[insert: **complete name of Supplier which in the case of a joint venture shall be in the name of the joint venture**]* (hereinafter called "the Applicant"). Furthermore, we understand that, according to the conditions of the Contract, a performance guarantee is required.

At the request of the Applicant , we as Guarantor hereby irrevocably undertake to pay you any sum(s) not exceeding *[insert: **amount(s)**[1] **in figures and words**]* such sum being payable in the types and proportions of currencies which the Contract Price is payable upon receipt by us of the Beneficiary's statement, whether in the demand itself or in a separate signed document accompanying or identifying the demand, stating that the Applicant is in breach of its obligation(s) under the contract without the Beneficiary needing to prove or to show grounds or reasons for their demand or the sum specified therein.

On the date of your issuing, to the Supplier, the Operational Acceptance Certificate for the System, the value of this guarantee will be reduced to any sum(s) not exceeding *[insert: **amount(s)**[1] **in figures and words**]*. This remaining guarantee shall expire no later than *[insert: **number** and select: **of months/of years** (of the Warranty Period that needs to be covered by the*

[1] *The bank shall insert the amount(s) specified and denominated in the SCC for GC Clauses 13.3.1 and 13.3.4 respectively, either in the currency(ies) of the Contract or a freely convertible currency acceptable to the Purchaser.*

remaining guarantee)] from the date of the Operational Acceptance Certificate for the System,[1] and any demand for payment under it must be received by us at this office on or before that date.

This guarantee is subject to the Uniform Rules for Demand Guarantees, (URDG) 2010 Revision, ICC Publication No. 758, except that the supporting statement under 15 (a) is hereby excluded.

_____

[Signature(s)]

Note: All italicized text (including footnotes) is for use in preparing this form and shall be deleted from the final product.

[1] *In this sample form, the formulation of this paragraph reflects the usual SCC provisions for GC Clause 13.3. However, if the SCC for GC Clauses 13.3.1 and 13.3.4 varies from the usual provisions, the paragraph, and possibly the previous paragraph, need to be adjusted to precisely reflect the provisions specified in the SCC.*

2.2 Advance Payment Security
Bank Guarantee

_____

[Guarantor letterhead or SWIFT identifier code]

Beneficiary: *[insert: **Name and Address of Purchaser**]*

Date: *[**insert date of issue**]*

ADVANCE PAYMENT GUARANTEE No.: *[insert: **Advance Payment Guarantee Number**]*

Guarantor: *[Insert name and address of place of issue, unless indicated in the letterhead]*

We have been informed that on *[insert: **date of award**]* you awarded Contract No. *[insert: **Contract number**]* for *[insert: **title and/or brief description of the Contract**]* (hereinafter called "the Contract") to *[insert: **complete name of Supplier, which in the case of a joint venture shall be the name of the joint venture**]* (hereinafter called "the Applicant").

Furthermore, we understand that, according to the conditions of the Contract, an advance payment in the sum of ***[insert: amount in numbers and words, for each currency of the advance payment]*** is to be made to the Supplier against an advance payment guarantee.

At the request of the Applicant, we as Guarantor, hereby irrevocably undertake to pay the Beneficiary any sum or sums not exceeding in total an amount of *[insert amount in figures]* (_____) *[insert amount in words]*[1] upon receipt by us of the Beneficiary's complying demand supported by the Beneficiary's statement, whether in the demand itself or in a separate signed document accompanying or identifying the demand, stating either that the Applicant:

(a) has used the advance payment for purposes other than toward delivery of Goods; or

(b) has failed to repay the advance payment in accordance with the Contract conditions, specifying the amount which the Applicant has failed to repay.

[1] *The Guarantor shall insert an amount representing the amount of the advance payment and denominated either in the currency(ies) of the advance payment as specified in the Contract, or in a freely convertible currency acceptable to the Purchaser.*

A demand under this guarantee may be presented as from the presentation to the Guarantor of a certificate from the Beneficiary's bank stating that the advance payment referred to above has been credited to the Applicant on its account number *[insert number]* at *[insert name and address of Applicant's bank]*.

The maximum amount of this guarantee shall be progressively reduced by the amount of the advance payment repaid by the Applicant as specified in copies of interim statements or payment certificates which shall be presented to us. This guarantee shall expire, at the latest, upon our receipt of a copy of the interim payment certificate indicating that ninety (90) percent of the Accepted Contract Amount, has been certified for payment, or on the *[insert day]* day of *[insert month]*, 2 *[insert year]*, whichever is earlier. Consequently, any demand for payment under this guarantee must be received by us at this office on or before that date.

This guarantee is subject to the Uniform Rules for Demand Guarantees (URDG) 2010 Revision, ICC Publication No.758, except that the supporting statement under Article 15(a) is hereby excluded.

.

_____

[signature(s)]

Note: All italicized text (including footnotes) is for use in preparing this form and shall be deleted from the final product.

3. Installation and Acceptance Certificates

3.1 Installation Certificate

Date: ***[insert: date]***

Loan/Credit Number: ***[insert: loan or credit number from RFB]***

RFB: ***[insert: title and number of RFB]***

Contract: ***[insert: name and number of Contract]***

To: ***[insert: name and address of Supplier]***

Dear Sir or Madam:

Pursuant to GCC Clause 26 (Installation of the System) of the Contract entered into between yourselves and the ***[insert: name of Purchaser]*** (hereinafter the "Purchaser") dated ***[insert: date of Contract],*** relating to the ***[insert: brief description of the Information System],*** we hereby notify you that the System (or a Subsystem or major component thereof) was deemed to have been correctly installed on the date specified below.

1. Description of the System (or relevant Subsystem or major component: ***[insert: description]***

2. Date of Installation: ***[insert: date]***

Notwithstanding the above, you are required to complete the outstanding items listed in the attachment to this certificate as soon as practicable. This letter shall not relieve you of your obligation to achieve Operational Acceptance of the System in accordance with the Contract nor of your obligations during the Warranty Period.

For and on behalf of the Purchaser

Signed:

Date:

in the capacity of: ***[state: "Project Manager" or state the title of a higher level authority in the Purchaser's organization]***

3.2 Operational Acceptance Certificate

Date: ***[insert: date]***

Loan/Credit Number: ***[insert: loan or credit number from RFB]***

RFB: ***[insert: title and number of RFB]***

Contract: ***[insert: name of System or Subsystem and number of Contract]***

To: ***[insert: name and address of Supplier]***

Dear Sir or Madam:

Pursuant to GCC Clause 27 (Commissioning and Operational Acceptance) of the Contract entered into between yourselves and the ***[insert: name of Purchaser]*** (hereinafter the "Purchaser") dated ***[insert: date of Contract],*** relating to the ***[insert: brief description of the Information System],*** we hereby notify you the System (or the Subsystem or major component identified below) successfully completed the Operational Acceptance Tests specified in the Contract. In accordance with the terms of the Contract, the Purchaser hereby takes over the System (or the Subsystem or major component identified below), together with the responsibility for care and custody and the risk of loss thereof on the date mentioned below.

1. Description of the System (or Subsystem or major component): ***[insert: description]***

2. Date of Operational Acceptance: ***[insert: date]***

This letter shall not relieve you of your remaining performance obligations under the Contract nor of your obligations during the Warranty Period.

For and on behalf of the Purchaser

Signed:

Date:

in the capacity of: ***[state: "Project Manager" or higher level authority in the Purchaser's organization]***

4. CHANGE ORDER PROCEDURES AND FORMS

Date: ***[insert: date]***

Loan/Credit Number: ***[insert: loan or credit number from RFB]***

RFB: ***[insert: title and number of RFB]***

Contract: ***[insert: name or System or Subsystem and number of Contract]***

General

This section provides samples of procedures and forms for carrying out changes to the System during the performance of the Contract in accordance with GCC Clause 39 (Changes to the System) of the Contract.

Change Order Log

The Supplier shall keep an up-to-date Change Order Log to show the current status of Requests for Change and Change Orders authorized or pending. Changes shall be entered regularly in the Change Order Log to ensure that the log is kept up-to-date. The Supplier shall attach a copy of the current Change Order Log in the monthly progress report to be submitted to the Purchaser.

References to Changes

(1) Request for Change Proposals (including Application for Change Proposals) shall be serially numbered CR-nnn.
(2) Change Estimate Proposals shall be numbered CN-nnn.
(3) Estimate Acceptances shall be numbered CA-nnn.
(4) Change Proposals shall be numbered CP-nnn.
(5) Change Orders shall be numbered CO-nnn.

On all forms, the numbering shall be determined by the original CR-nnn.

Annexes

4.1 Request for Change Proposal Form
4.2 Change Estimate Proposal Form
4.3 Estimate Acceptance Form
4.4 Change Proposal Form
4.5 Change Order Form
4.6 Application for Change Proposal Form

4.1 Request for Change Proposal Form

(Purchaser's Letterhead)

Date: ***[insert: date]***

Loan/Credit Number: ***[insert: loan or credit number from RFB]***

RFB: ***[insert: title and number of RFB]***

Contract: ***[insert: name of System or Subsystem or number of Contract]***

To: ***[insert: name of Supplier and address]***

Attention: ***[insert: name and title]***

Dear Sir or Madam:

With reference to the above-referenced Contract, you are requested to prepare and submit a Change Proposal for the Change noted below in accordance with the following instructions within ***[insert: number]*** days of the date of this letter.

1. Title of Change: ***[insert: title]***

2. Request for Change No./Rev.: ***[insert: number]***

3. Originator of Change: ***[select Purchaser / Supplier (by Application for Change Proposal), and add: name of originator]***

4. Brief Description of Change: ***[insert: description]***

5. System (or Subsystem or major component affected by requested Change): ***[insert: description]***

6. Technical documents and/or drawings for the request of Change:

   Document or Drawing No. Description

7. Detailed conditions or special requirements of the requested Change: ***[insert: description]***

8. Procedures to be followed:

   (a) Your Change Proposal will have to show what effect the requested Change will have on the Contract Price.

   (b) Your Change Proposal shall explain the time it will take to complete the requested Change and the impact, if any, it will have on the date when Operational Acceptance of the entire System agreed in the Contract.

   (c) If you believe implementation of the requested Change will have a negative impact on the quality, operability, or integrity of the System, please provide a detailed explanation, including other approaches that might achieve the same impact as the requested Change.

   (d) You should also indicate what impact the Change will have on the number and mix of staff needed by the Supplier to perform the Contract.

   (e) You shall not proceed with the execution of work related to the requested Change until we have accepted and confirmed the impact it will have on the Contract Price and the Implementation Schedule in writing.

9. As next step, please respond using the Change Estimate Proposal form, indicating how much it will cost you to prepare a concrete Change Proposal that will describe the proposed approach for implementing the Change, all its elements, and will also address the points in paragraph 8 above pursuant to GCC Clause 39.2.1. Your Change Estimate Proposal should contain a first approximation of the proposed approach, and implications for schedule and cost, of the Change.

For and on behalf of the Purchaser

Signed:

Date:

in the capacity of: ***[state: "Project Manager" or higher level authority in the Purchaser's organization]***

4.2 Change Estimate Proposal Form

(Supplier's Letterhead)

Date: ***[insert: date]***

Loan/Credit Number: ***[insert: loan or credit number from RFB]***

RFB: ***[insert: title and number of RFB]***

Contract: ***[insert: name of System or Subsystem and number of Contract]***

To: ***[insert: name of Purchaser and address]***

Attention: ***[insert: name and title]***

Dear Sir or Madam:

With reference to your Request for Change Proposal, we are pleased to notify you of the approximate cost of preparing the below-referenced Change in accordance with GCC Clause 39.2.1 of the Contract. We acknowledge that your agreement to the cost of preparing the Change Proposal, in accordance with GCC Clause 39.2.2, is required before we proceed to prepare the actual Change Proposal including a detailed estimate of the cost of implementing the Change itself.

1. Title of Change: ***[insert: title]***

2. Request for Change No./Rev.: ***[insert: number]***

3. Brief Description of Change (including proposed implementation approach): ***[insert: description]***

4. Schedule Impact of Change (initial estimate): ***[insert: description]***

5. Initial Cost Estimate for Implementing the Change: *[insert:* ***initial cost estimate****]*

6. Cost for Preparation of Change Proposal: ***[insert: cost in the currencies of the Contract],*** as detailed below in the breakdown of prices, rates, and quantities.

For and on behalf of the Supplier

Signed:

Date:

in the capacity of: ***[state: "Supplier's Representative" or other higher level authority in the Supplier's organization]***

4.3 Estimate Acceptance Form

(Purchaser's Letterhead)

Date: ***[insert: date]***

Loan/Credit Number: ***[insert: loan or credit number from RFB]***

RFB: ***[insert: title and number of RFB]***

Contract: ***[insert: name of System or Subsystem and number of Contract]***

To: ***[insert: name of Supplier and address]***

Attention: ***[insert: name and title]***

Dear Sir or Madam:

We hereby accept your Change Estimate and agree that you should proceed with the preparation of a formal Change Proposal.

1. Title of Change: ***[insert: title]***

2. Request for Change No./Rev.: ***[insert: request number / revision]***

3. Change Estimate Proposal No./Rev.: ***[insert: proposal number / revision]***

4. Estimate Acceptance No./Rev.: ***[insert: estimate number / revision]***

5. Brief Description of Change: ***[insert: description]***

6. Other Terms and Conditions:

In the event that we decide not to order the Change referenced above, you shall be entitled to compensation for the cost of preparing the Change Proposal up to the amount estimated for this purpose in the Change Estimate Proposal, in accordance with GCC Clause 39 of the General Conditions of Contract.

For and on behalf of the Purchaser

Signed:

Date:

in the capacity of: ***[state: "Project Manager" or higher level authority in the Purchaser's organization]***

4.4 Change Proposal Form

(Supplier's Letterhead)

Date: ***[insert: date]***

Loan/Credit Number: ***[insert: loan or credit number from RFB]***

RFB: ***[insert: title and number of RFB]***

Contract: ***[insert: name of System or Subsystem and number of Contract]***

To: ***[insert: name of Purchaser and address]***

Attention: ***[insert: name and title]***

Dear Sir or Madam:

In response to your Request for Change Proposal No. ***[insert: number],*** we hereby submit our proposal as follows:

1. Title of Change: ***[insert: name]***

2. Change Proposal No./Rev.: ***[insert: proposal number/revision]***

3. Originator of Change: ***[select: Purchaser / Supplier; and add: name]***

4. Brief Description of Change: ***[insert: description]***

5. Reasons for Change: ***[insert: reason]***

6. The System Subsystem, major component, or equipment that will be affected by the requested Change: ***[insert: description]***

7. Technical documents and/or drawings for the requested Change:

   Document or Drawing No. Description

8. Estimate of the increase/decrease to the Contract Price resulting from the proposed Change: ***[insert: amount in currencies of Contract],*** as detailed below in the breakdown of prices, rates, and quantities.

   Total lump sum cost of the Change:

   Cost to prepare this Change Proposal (i.e., the amount payable if the Change is not accepted, limited as provided by GCC Clause 39.2.6):

9. Additional Time for Achieving Operational Acceptance required due to the Change: ***[insert: amount in days / weeks]***

10. Effect on the Functional Guarantees: ***[insert: description]***

11. Effect on the other terms and conditions of the Contract: ***[insert: description]***

12. Validity of this Proposal: for a period of ***[insert: number]*** days after receipt of this Proposal by the Purchaser

13. Procedures to be followed:

    (a) You are requested to notify us of your acceptance, comments, or rejection of this detailed Change Proposal within ***[insert: number]*** days from your receipt of this Proposal.

    (b) The amount of any increase and/or decrease shall be taken into account in the adjustment of the Contract Price.

For and on behalf of the Supplier

Signed:

Date:

in the capacity of: ***[state: "Supplier's Representative" or other higher level authority in the Supplier's organization]***

4.5 Change Order Form

(Purchaser's Letterhead)

Date: ***[insert: date]***

Loan/Credit Number: ***[insert: loan or credit number from RFB]***

RFB: ***[insert: title and number of RFB]***

Contract: ***[insert: name of System or Subsystem and number of Contract]***

To: ***[insert: name of Supplier and address]***

Attention: ***[insert: name and title]***

Dear Sir or Madam:

We hereby approve the Change Order for the work specified in Change Proposal No. ***[insert: number]***, and agree to adjust the Contract Price, Time for Completion, and/or other conditions of the Contract in accordance with GCC Clause 39 of the Contract.

1. Title of Change: ***[insert: name]***

2. Request for Change No./Rev.: ***[insert: request number / revision]***

3. Change Order No./Rev.: ***[insert: order number / revision]***

4. Originator of Change: ***[select: Purchaser / Supplier; and add: name]***

5. Authorized Price for the Change:

   Ref. No.: ***[insert: number]*** Date: ***[insert: date]***

   [insert: amount in foreign currency A] plus ***[insert: amount in foreign currency B]*** plus ***[insert: amount in foreign currency C]*** plus ***[insert: amount in local currency]***

6. Adjustment of Time for Achieving Operational Acceptance: ***[insert: amount and description of adjustment]***

7. Other effects, if any: ***[state: "none" or insert description]***

For and on behalf of the Purchaser

Signed:

Date:

in the capacity of: ***[state: "Project Manager" or higher level authority in the Purchaser's organization]***

For and on behalf of the Supplier

Signed:

Date:

in the capacity of: ***[state "Supplier's Representative" or higher level authority in the Supplier's organization]***

4.6 Application for Change Proposal Form

(Supplier's Letterhead)

Date: ***[insert: date]***

Loan/Credit Number: ***[insert: loan or credit number from RFB]***

RFB: ***[insert: title and number of RFB]***

Contract: ***[insert: name of System or Subsystem and number of Contract]***

To: ***[insert: name of Purchaser and address]***

Attention: ***[insert: name and title]***

Dear Sir or Madam:

We hereby propose that the below-mentioned work be treated as a Change to the System.

1. Title of Change: ***[insert: name]***

2. Application for Change Proposal No./Rev.: ***[insert: number / revision]*** dated: ***[insert: date]***

3. Brief Description of Change: ***[insert: description]***

4. Reasons for Change: ***[insert: description]***

5. Order of Magnitude Estimation: ***[insert: amount in currencies of the Contract]***

6. Schedule Impact of Change: ***[insert: description]***

7. Effect on Functional Guarantees, if any: ***[insert: description]***

8. Appendix: ***[insert: titles (if any); otherwise state "none"]***

For and on behalf of the Supplier

Signed:

Date:

in the capacity of: ***[state: "Supplier's Representative" or higher level authority in the Supplier's organization]***