DRAFT

Terms of Reference (TOR)
For
Development of cyber security strategy, assessment of critical infrastructure, provision of self-assessment toolkit, and basic cyber security package for agencies (Package #AF-S3)

1. Background

Government of Bangladesh requires strategic cyber oversight of Critical Information Infrastructures (CII) by developing, deploying and maintaining coordinated cyber visibility across CII organizations. Development of cyber strategy, risk assessment framework and provision of related tools will allow for Government of Bangladesh to govern CII in cyber security area and will contribute to raising cyber maturity level across CII organizations.

2. Objectives

With unprecedented frequency of breaches and levels of security spending, GOB considers cyber security less as a resource burden or technology discipline, but a country wide risk strategy and foundation for economic viability. In this regard the National Cyber Security Strategy, which has been ratified in March, 2014 needs to be revisited and enhanced to secure a better future for the citizens of Bangladesh.

The first objective of this assignment is to revise and enhance the National Cyber Security Strategy with key focus on the following four pillars, which should underpin the National Cyber Security Strategy.

- Strengthening resilience of Critical Information Infrastructures (CIIs).
- Mobilizing businesses and the community to make cyber space safer, by countering cyber threats, combating cybercrime and protecting personal data.
- Developing a vibrant cyber security ecosystem comprising a skilled workforce, technologically advanced companies and strong research collaborations, so that it can support country's cybersecurity needs and be a source of new economic growth.
- Stepping up efforts to forge strong international partnerships.

GOB takes into account Cyber Security as a Core Enabler in Critical Infrastructure Resilience and Growth, so with strategic key focus on **Safeguarding Critical Infrastructure, the second objective is** to develop cyber security strategy and establish comprehensive cyber security risk assessment framework to govern cyber security risks for CII. Based on that, to implement related information systems and to enable CIIs to use them to manage cyber risks and ensure compliance with applicable laws and regulations.

3. Scope of Work

3.1 Review and Enhancement of National Cyber Security Strategy, 2014. To review and enhance National Cyber Security Strategy of Bangladesh, 2014. The National Cyber security

Strategy must include vision, goals and priorities of GOB. The National Cyber Security Strategy must focus on the following:

- Protection of Essential Services
- Responding Decisively to Cyber Threats
- Strengthening Governance and Legislative Framework
- Securing Government Networks
- Forging International and Regional Cooperation to Counter Cyber Threats and Cybercrime
- Facilitating International and Regional Exchanges on Cyber Norms and Legislation
- Establishing a Professional Cyber security Workforce
- Promoting Innovation to Accelerate
- Combating Cybercrime
- Promoting Collective Responsibility

3.2. Development of cyber security strategy for CII. Conduct review of the relevant measures for cyber security applicable to CII, including institutional, procedural, and technical, and based on the international best practice and/or selected framework to prepare cyber security development strategy for CII with actionable master plan. Activities shall include interviews with relevant stakeholders and CII owners. Cyber security strategy shall contain:

- Vision and mission of the government to secure its CII networks, applications and data;
- legal and regulatory measures for cyber security in CII;
- A lead government agency to be responsible for supervising cyber security activities in CII;
- Roles and responsibilities assigned to respective government agencies, including framework for cooperation within government, private sector, and internationally;
- Financial estimation for proposed master plan implementation.

3.3. Preparation of Cyber risk assessment framework. Framework shall contain at least asset identification, customizable threat list selection model, entering vulnerabilities, probability and impact scoring, risks scenarios, and risk treatment activities. International best practices on risk management have to be incorporated into the cyber risk assessment framework. Proposed framework has to ensure tractability of data calculated and data re-usage. In this regard the purchaser suggests reviewing existing risk assessment frameworks like NIST Cyber Security Risk Assessment Framework and COSO Enterprise Risk Management Framework, and NERC Cyber Security Standards Risk Based Methodology and conceptualizing them in the context of Bangladesh.

3.4. Implementation guidelines for cyber risk assessment framework and compliance management. Guidelines shall contain consideration on how proposed risk assessment framework has to be incorporated into CII governance and enterprise risk management (ERM) processes, what kind of outputs should be taken into CII governance and cyber strategy development activities. It should consider what kind of organizational entities must be established in order to support execution of the framework. The document should also suggest how organizations have to manage compliance to regulatory requirements and how risk and compliance management activities fits together and produce comparable results.

3.5. Cyber risk assessment of selected CIIs. Consultant has to implement and execute Cyber risk assessment framework at three (3) selected Critical Information Infrastructures from different sectors. National Data Center (NDC), located at Bangladesh Computer Council (BCC) would be one of them. Other two (2) Critical Infrastructures would be selected from Financial and Utility sectors respectively. Complete details of the selected Critical Information Infrastructures would be provided to the winning bidder on signing a Non-disclosure Agreement (NDA) after issuance of notification of award (NOA). Implementation of cyber risk assessment framework at the selected infrastructures from different sectors must prove the capabilities of the framework. The framework and guidelines must be updated according to the findings, comments, and issues found/received during the risk assessment of CIIs.

3.6. Establishment of information system for cyber risk assessments and compliance management (CRACM). Proposed cyber risk assessment framework shall be incorporated into the information system (CRACM). CRACM has to ensure compliance management activities to various local, international, and custom requirements. The system should be accessible for all CII within GoB. Information system will be placed and hardware resources will be given by the National Data Centre. CRACM should allow data export capabilities in a raw (CSV, and database access via ODBC or RESTful API) and human readable (docx or pdf) formats. In case of custom development source code should be provided to the Bangladesh Computer Council. In case of licensed CRACM version 3 years license should be provided for at least 100 users. Previous CII assessment results (see section 0) should be incorporated into the CRACM tool. CRACM shall ensure Two (2) Factor strong authentications and be compatible with 4 major browsers: IE, Chrome, Safari, and Firefox. CRACM should comply with applicable GoB's information security requirements found in GOBISM. (http://www.bcc.gov.bd/site/notices/c3e4eb26-7f3a-4b5d-a9da-b18f40a9598b/Government-of-bd-Information-Security-Manual).CRACM would be a self-contained software tool. It would evaluate the cyber security of an automated, industrial control or business system using a hybrid risk and standards-based approach, and would provide relevant recommendations for improvement. CRACM would help asset owners to assess their information and operational systems cyber security practices by asking a series of detailed questions about system components and architecture, as well as operational policies and procedures. These questions would be derived from accepted industry cybersecurity standards.

Once the self-assessment questionnaire is complete, CRACM would provide a prioritized list of recommendations for increasing cyber security posture, including solutions; common practices, compensating actions, and component enhancements or additions. The tool would also identify what is needed to achieve a desired level of cyber security within a system's specific configurations. CRACM must be able to determine security assurance level (SAL) by responses to questions relating to the potential consequences of a successful cyber attack on a CII organization, facility, system, or subsystem. CRACM would then calculate a SAL and would provide a recommended level of cyber security rigor necessary to protect against a worst-case event. Using the SAL to determine the required level of security, CRACM would run a comparative analysis between the requirements identified in the standards selected and the answers provided by the user.

CRACM would contain a graphical user interface that would allow one to diagram the control system network topology and identify the "criticality" of the network components. By creating a network architecture diagram, users would be able to define the organization's

cyber security zones, critical components, and communications conduits. An icon palette featuring various system and network components would allow users to build diagrams by simply dragging and dropping them into place. Specific questions would further facilitate the detailed identification of each component. CRACM would then generate questions using the network topology and selected security standards, risk management frameworks as its basis. The assessment team would select the best answer to each question using the organization's actual network configuration and implemented security policies and procedures. The tool would compare the completed answers with the recommended requirements from the standards and would generate a list of risks, security gaps and recognized good practices. CRACM would also generate both interactive (on-screen) and printed reports. The reports would provide a summary of risks, likelihood and impact of risks, security level gaps or areas that did not meet the recommendations of the selected standards. The assessment team may then use this information to plan and prioritize mitigation strategies.

3.7. "How to" trainings. Up to five "How to" training sessions on CII cyber risk assessment framework and use of CRACM has to be conducted to the management and staff of the selected CIIs.

3.8. CRACM deployment and support. Established information system must be deployed to all selected CIIs in parallel with "How to" trainings and maintenance (software errors resolution and patching) for 6 (six) months after deployment.

3.9. Reporting and Time Schedules

SL #	Deliverable	Timing (Months after commencement of the Contract)
1	Inception Report	1
2	Review and Enhancement of National Cyber Security Strategy, 2014 (as per 3.1)	2
3	Cyber security strategy and actionable master plan for CII (as per 3.2)	3
4	Cyber risk assessment framework (as per 3.3)	4
5	Implementation guidelines for cyber risk assessment framework and compliance management (as per 3.4)	5
6	Cyber risk assessment of National Data Center and two other selected critical information infrastructures (as per 3.5)	6
7	Cyber risk assessment of National Data Center and two other selected critical information infrastructures (as per 3.6)	7
8	"How to" trainings (as per 3.7)	8-12
9	CRACM deployment (as per 3.8)	8-12
10	CRACM support (as per 3.8)	8-12

4. Local Implementation Partner

In Bangladesh, a Consultant will work in a close partnership with a local company which will be its local implementation partner. The host institution will provide support in all stages of project's execution.

5. Warranty

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

5.1. Warranty Services: 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.

5.2. 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.

6. Qualification and Experience of Firm

FIRM

- Leading information security organization with at least one reference in each area:
  - IT/information/cyber security governance model or strategy, or action plan preparation and delivery to government or government's organization
  - Information/cyber security risk assessment/critical information infrastructure identification methodology preparation and delivery to government or government's organization
- Demonstrated capability in design, development and delivery of information security policies, standards and guidelines related to the IT domain.
- The firm must have proven CRACM implementation track record (documentary evidence must be submitted).

7. Consultant Team

Key Professional Staff:

(1) Team leader:

At least master's degree in IT or consulting with minimum 10 years' experience in a leadership role in designing and deploying national level information security policies, regulations, standards and guidelines for at least one country. The team leader should have ISACA/EC Council/SANS or related professional certification in area of information/cyber security risk management. [1 Person-12 person months]

(2) Project manager:

At least master's degree in IT or project management with minimum 10 years' experience in IT and 5 years in information security fields. He/she should have

international project management experience in consulting projects related to IT or IT security. [1Person-12 person months]

(3) Legal lead adviser:

At least a master's degree in law with minimum 5 years' experience in law practice and 3 years' experience in information security. He/she should have governance or strategy consulting and/or Information/cyber security risk assessment/critical information infrastructure identification methodology preparation practice. [1 person - 06 person months]

(4) Software lead architect:

At least a bachelor's degree in IT or Computer Science with minimum 5 years' experience in secure and layered software architecture including browser agnostic web technologies. [1 person-06 person months]

All the key experts mentioned above must have international experience (one country outside his/her home Country).
Total key-professional staff effort is estimated at **36 person-months.**

Non-Key Professional Staff:

In addition to key experts the following non-key experts may be required to deliver the service in accordance to the TOR. Indicative list of non-key experts is given below as a guideline for the bidders. However, the potential bidders are free to make their own estimate in proposing non-key experts. CVs of the proposed non-key professional staff should be provided.

a. Information security expert
b. Network engineer
c. Hardware engineer
d. Application developer
e. Quality assurance/test specialist
f. Systems administrator
g. Systems engineer
h. Lawyer with experience in information security

8. Counterpart facilities

The project will provide institutional support and all available documents, data and information to the Consultant after signing a Non-disclosure Agreement (NDA) after issuance of Notification of Award. The Consultant should include all eligible expenditure in the financial proposal for accommodation, logistics and required manpower for successful implementation of the assignment.

9. Payment Schedule

The payment schedule will be as follows:

- Ten (10) percent of the contracted amount will be paid upon submission and acceptance of Inception Report by the client after 1 month from the commencement date of contract.

- Ten (10) percent of the contracted amount will be paid upon submission and acceptance of the report after completing the works (according to section 3.1), that is "Review and Enhancement of National Cyber Security Strategy, 2014" within 2 month from the commencement date of contract.
- Five (5) percent of the contracted amount will be paid upon submission of Cyber security strategy and actionable master plan for CII (according to section 3.2) report and acceptance of it by the client within 3 months from the commencement date of contract.
- Five (5) percent of the contracted amount will be paid upon submission Cyber risk assessment framework (according to section 3.3) report and acceptance of it by the client within 4 months from the commencement date of contract.
- Ten (10) percent of the contracted amount will be paid upon submission of Implementation guidelines for cyber risk assessment framework and compliance management (according to section 3.4) report and acceptance of it by the client within 5 months from the commencement date of contract.
- Ten (10) percent of the contracted amount will be paid upon submission of Cyber risk assessment of National Data Center (according to section 3.5) report and acceptance of it by the client within 6 months from the commencement date of contract.
- Ten (10) percent of the contracted amount will be paid upon submission of Establishment of information system for cyber risk assessments and compliance management (CRACM) (according to section 3.6) report and acceptance of it by the client within 7 months from the commencement date of contract.
- Ten (10) percent of the contracted amount will be paid upon submission of "How to" trainings (according to section 3.7) report and acceptance of it by the client within 10 months from the commencement date of contract.
- Fifteen (15) percent of the contracted amount will be paid upon submission of CRACM deployment (according to section 3.8) report and acceptance of it by the client within 11 months from the commencement date of contract.
- Fifteen (15) percent of the contracted amount will be paid upon submission of CRACM support (according to section 3.8) report and acceptance of it by the client within 12 months from the commencement date of contract.

10. Duration

The entire consultancy work including submission of CRACM system, reports, documents etc. according to this terms of reference (TOR) shall be completed within 12 (twelve) months from the commencement date.