DRAFT

Terms of Reference
for
Enhancement of Incident response capabilities of BGD e-GOV CIRT
(Package #AF-S4)

1. Background

In July 2015, Bangladesh Computer Council (BCC) under the Ministry of Posts, Telecommunications & Information Technology has signed the contract to enable incident handling capabilities by establishing Computer Incident Response Team (CIRT). As a result of the project implementation, BCC acquired the necessary technology, established processes: cyber security incident handling, security assessments, intrusion detection, security consulting, awareness building, and developed skills needed to run and maintain CIRT. CIRT has also been introduced to international CIRT community and became a member of the Forum of Incident Response and Security Teams (FIRST.Org), OIC-CERT, pending member of APCERT. The mandate which describes CIRT obligations and responsibilities was upgraded in just 6 months after the CIRT establishment, currently allowing the unit to act as a Bangladesh Government Computer Incident Response Team (BGD e-GOV CIRT). More information about CIRT activities is provided in the webpage www.cirt.gov.bd .

However, as BGD e-GOV CIRT is still in infancy stage, its further successful operations and service delivery largely depend on continuous support from internal and external parties. There is a risk of annulling the progress made so far if the external assistance and support in current dynamic environment is removed too early.

2. Objectives of the Assignment

The objective of this assignment is to support BGD e-GOV CIRT organisation in the following areas according to the BGD e-GOV CIRT development plan:

i. **Organisation processes**
Strengthening, by improving maturity of processes and enhancing automation and protection;

ii. **CIRT services portfolio**
Expansion, by provisioning additional services to constituency;

iii. **Operational environments of constituency**
Clarification of requirements, by setting technical hygiene level for hosting and classification of information levels;

3. Scope of Services

The following activities have to be performed during the project.

1. Under “I. Strengthening organisation processes”:
   1.1. CIRT certification according CIRT SIM3 maturity model
   1.2. Advancing CIRT systems and structure
   1.3. Automation of incident handling
2. Under **“**II. Expanding CIRT services portfolio”:
   2.1. New service: Technical Cyber security Assessment
   2.2. New service: Information Sharing and Publications

2.3. New service: Vulnerability Advisory

2.4. New service: Promoting Cyber security

2.5. Enlarging service delivery capacity

3. Under **"**III. Clarifying requirements for the operational environments of constituency":

3.1. Ensuring security compliance for new IT systems deployable to NDC

3.2. Manual on cyber security controls for classified information

4. Under "Project Administration":

4.1. Inception Report

4.2. Project Monthly Progress Reports

4.3. Closing Report

Detail activity descriptions, timeline and outcomes are provided below. Timeline marks the activity beginning and finish milestones comparing from the project start.

1. Under "I. Strengthening organisation processes":

1.1. BGD e-GOV CIRT certification according CSIRT SIM3 maturity model

Consultant must conduct BGD e-GOV CIRT processes maturity assessment and validation, identify mandatory improvements to pass the SIM3 certification process, and facilitate all the improvements needed. Consultant must organise and run the certification process until full certification status.

1.2. Advancing CIRT systems and structure

Consultant must manage (plan, coordinate implementation, do software and systems integrations and development) modernisation of BGD e-GOV CIRT via:

(i) introduction of modern 2nd factor authentication for CIRT staff for more efficient and secure work as well as operational tuning of existing systems for optimal use;

(ii) introducing CIRT continuous integration process for changes in CIRT infrastructure, separation CIRT core systems development, testing, and production environments, including systems deployment automation;

(iii) facilitation collaboration with CIRT community worldwide by setting up two platforms of automated sharing locally-developed cyber threat intelligence (indicators and detected attack information) with global CIRT trusted communities; the platforms have to be reputable and already used in similar information sharing capacity in other CIRT environments;

(iv) introduce additional tactical security assessment and analysis tools into CIRT processes In order to provide capabilities to CIRT team to analyse, and validate methods and techniques used by attackers;

(v) increase the quality (reduce false positives, aggregate and enhance the attributes of data for relevance of served constituency) of threat intelligence data and start automatically provisioning of such data to the constituents;

(vi) improving BGD e-GOV CIRT website platform with new functionalities for reporting, publishing, automation and access. Integration with reputation service to indicate that visitor comes from infected system.

1.3. Automation of incident handling

Currently incident attributes (IP addresses relationship with owner, administrator, and organisational structures) are handled manually at NDC and CIRT while processed via tracking system. Consultant must establish cyber inventory database (CIDB) and log archival solution at CIRT infrastructure needed for automation of such relationships in incident handling processes. Consultant must automate incident handling process integration of CIDB with CIRT tracking server and National Data Center service delivery and support processes. Consultant must similarly integrate with at least two other constituency organisations.

2. Under "II. Expanding CIRT services portfolio":

2.1. New service: Technical Cyber security Assessment

Consultant must design and implement (prepare documentation, train CIRT staff) CIRT service and processes for "Technical Cyber security Assessment" to be delivered by CIRT team on request by constituency. This service results should provide assessment on vulnerability level of constituency's IT hardware and software infrastructures, and must include at least automated scanning, human penetration testing and social engineering.

2.2. New service: Information Sharing and Publications

Consultant must design and implement (prepare documentation, train CIRT staff) CIRT service and affiliated service delivery process of "Information Sharing and Publications". After it is designed and implemented, Consultant must assist in creating at least 15 high-quality localised content articles to be published on website and promoted via public relations channels.

2.3. New service: Vulnerability Advisory

Consultant must design and implement (prepare documentation, train CIRT staff) CIRT service and processes of "Vulnerability Advisory". Consultant must introduce automated alerting on vulnerabilities related to constituents' assets and their criticality, provide system for weekly/monthly vulnerability briefs. Constituents must be able to subscribe advisories, configure assets, and mailing frequency. CIRT statistics reveal that numerous incidents are caused by exploiting known vulnerabilities. BGD e-GOV CIRT must react by introducing a new automated vulnerability warnings distribution service, which has to be prepared by the Consultant. Service will help the constituency to detect vulnerabilities on their assets as soon as these vulnerabilities are disclosed. Every constituency organization will have possibility to use email or web based self-service system where list of detected vulnerabilities of declared hardware and software will be emailed when noticed in the Common Vulnerabilities and Exposures database (MITRE CVE) or similar.

2.4. New service: Promoting Cyber security

BGD e-GOV CIRT recognition comes along with the responsibility to educate constituency on cyber resilience concepts as well as spread general cyber security awareness. The Consultant must support BGD e-GOV CIRT in organising a locally in Bangladesh event for CIRT worldwide community (in cooperation with FIRST.Org, APCERT, OIC-CERT or other relevant CIRT organization).

2.5. Enlarging service delivery capacity

BGD e-GOV CIRT is getting recognition among its constituency and at the same time, CIRT is starting to handle complex cyber security incidents. The crucial BGD e-GOV CIRT cyber investigations must be done utilising Consultant skills and experience for ensuring quality and speed. Consultant must also deliver legal and communication support when needed in

handling incidents. Assistance must include cyber security tools deployment, configuration, and maintenance during the incident. Consultant must provide within 1 working day access to key experts listed in proposal for at least 5 man-days non-interrupted access of engagement.

3. **Under "III. Clarifying requirements for the operational environments of constituency":**

3.1. Ensuring security compliance for new IT systems deployable to NDC

Currently there is a constant firefight in cyber security incidents handling in NDC. It is due to the lack of appropriate security management of applications by their owners, while hosting in NDC. To remediate the situation, Consultant must prepare easily enforceable and verifiable requirements for all applications, which are to be hosted at NDC in the form of applications on-boarding process at NDC, reducing the cyber security risks of NDC. Activity includes preparation of NDC security requirements ("baseline"), process and templates. Service must be replicable to other government organizations.

3.2. Manual on cyber security controls for classified information

Description of activity: There is no clear digital information sensitivity classification system with aligned protection requirements at the Client. This manifests in inefficiencies at CIRT work while handling incidents on inappropriately protected sensitive information. Consultant must prepare Manual on cyber security controls for classified information.

4. **Under "Project Administration":**

4.1. Project Inception Report

4.2. Project Monthly Progress Reports

4.3. Project Closing Report

4. Deliverables

The following table describes the deliverables of this assignment, which are the outputs of the activities specified under **Scope of Services.**

Note: T0 = Date of commencement of the Contract

SL. #	Deliverables	Submission Deadline (T1.1, T1.2, ….., TM.N)
1.	**Under "I. Strengthening organisation processes":**	
1.1	**BGD e-GOV CIRT SIM3 certification report** detailing certification successful process and providing relevant notes for future SIM3 model operation.	**T1.1 = T0 + 12 Month**
1.2	**Advancing CIRT systems and structure report,** showing that **e**ach (i) – (vi) sub-activities are accepted by CIRT team as complete.	**T1.2 = T0 + 15 Month**
1.3	**Automation of incident handling report,** confirming completion and: 1. Operational acceptance of deployed and integrated CIDB system; 2. Operational acceptance of the process integration of incident handling with NDC; 3. Operational acceptance of the process integration of incident handling with at least 2 (two) other organisations (outside NDC).	**T1.3 = T0 + 15 Month**
2.	**Under "II. Expanding CIRT services portfolio"**	
2.1	**Technical Cyber security Assessment Service Report**, covering: 1. prepared Service process documentation and operating procedures; 2. a proof that BGD e-GOV CIRT team successfully delivered at least	**T2.1 = T0 + 8 Month**

SL. #	Deliverables	Submission Deadline (T1.1, T1.2, ….., TM.N)
	two service instances according to the implemented process and procedures.	
2.2	**Information Sharing and Publications Service Report**, covering: 1. prepared Service process documentation and operating procedures; 2. a proof that BGD e-GOV CIRT team successfully delivered at least two service instances according to the implemented process and procedures; 3. a proof that there was written, published and promoted at least 15 articles, and their access rates are measured and analysed.	**T2.2 = T0 + 15 Month**
2.3	**Vulnerability Advisory Service Report,** covering: 1. prepared Service documentation; 2. a proof that service automation system is operational and providing service to at least three constituency teams.	**T2.3 = T0 + 6 Month**
2.4	**Promoting Cyber security Service Report,** covering: 1. prepared Service documentation; 2. a proof that at least one international conference locally was organised in partnership with international CSIRT association.	**T2.4 = T0 + 12 Month**
2.5	**Enlarging service delivery capacity Report** on utilisation of key experts for investigations used during all project, and amount of time was not less than 15 full working days	**T2.5 = T0 + 15 Month**
3.	**Under "III. Clarifying requirements for the operational environments of constituency"**	
3.1	**Security compliance for new IT systems deployable to NDC Report** covering: 1. accepted document package for the security requirements and processes on boarding applications at NDC; 2. proof of a successful process implementation by documenting at least two new on boarded IT systems according to this process.	**T3.1 = T0 + 12 Month**
3.2	**Manual on cyber security controls for classified information,** according to the Scope definition.	**T3.2 = T0 + 12 Month**
4.	**Under "Project Administration":**	
4.1.	**Project Inception Report,** which will contain the following: 1. Table of contents 2. List of abbreviations 3. Executive summary o General progress. o Work Plan o Assessment of the project objectives. o Problems encountered. - Problems or difficulties foreseen and their implications for future actions. The beneficiary should also provide an assessment to what extent these problems will affect the timely completion of the project, and describe the measures taken to overcome the problems in question. - If the project seems likely to become/stay behind schedule, please indicate this clearly. The beneficiary must signal changes to the baseline implementation programme. 4. Administrative	**T4.1 = T0 + 1 Month**

SL. #	Deliverables	Submission Deadline (T1.1, T1.2, ….., TM.N)
	4.1.Description of the Project Management 4.2.Organogram of the project team and the project management structure 5. Technical Please start with a few lines of your understanding about the project background and project adjectives 5.1. Actions 5.1.1. Action 1 5.1.2. Action 2 : 5.1.N. Action N - Describe what will be done regarding each action (and sub-action if applicable). For each of the objectives of the action, indicate whether you estimate you will achieve them. Where these objectives are quantitative, indicate the target, what you think you will achieve by the end of the project. Please present the plan of the project using a Gantt-chart or similar. 6. Envisaged progress until next report 7. Deliverables with indicators of final outputs. 8. Availability of appropriate human resources and their work schedule 9. Financial Part 9.1 Costs Elements (Incurred and estimated cost summary by cost category and relevant comments)**.** 10. Conclusion	
4.2.	**Project Monthly Progress Reports:** 1. Table of contents 2. List of abbreviations 3. Executive summary o Progress of the project o Problems encountered. - Problems or difficulties encountered and foreseen and their implications for future actions. The beneficiary should also provide an assessment to what extent these problems will affect the timely completion of the project, and describe the measures taken to overcome the problems in question. - If the project seems likely to become/stay behind schedule, please indicate this clearly. The beneficiary must signal changes to the baseline implementation programme. 4. Conclusion 5. Annexure	**T4.2.x = end of every month (2..14)**
4.3.	**Project Final Report** will include overview of all activities finished. Along with detailed final report a summary of the report in Microsoft Power Point format must be submitted.	**T4.3 = T0 + 15 month**

5. Reporting Arrangement

SL. #	Report Name	Report Format and Quantity	Submit To	To be reviewed by	Review and Response Time
1.1	BGD e-GOV CIRT SIM3 certification	(a) Softcopy(PDF) – 1 (b) Hardcopy – 1 (Presentable with	Project Director, Leveraging ICT	Leveraging ICT for Growth, Employment and	Two (2) weeks from the date of receiving the

SL. #	Report Name	Report Format and Quantity	Submit To	To be reviewed by	Review and Response Time
	report	excellent feel and look, paper size – A4)	for Growth, Employment and Governance Project	Governance Project	report
1.2	Advancing CIRT systems and structure report	(a) Softcopy(PDF) – 1 (b) Hardcopy – 1 (Presentable with excellent feel and look, paper size – A4)	Project Director, Leveraging ICT for Growth, Employment and Governance Project	Leveraging ICT for Growth, Employment and Governance Project	Two (2) weeks from the date of receiving the report
1.3	Automation of incident handling report .	(a) Softcopy(PDF) – 1 (b) Hardcopy – 1 (Presentable with excellent feel and look, paper size – A4)	Project Director, Leveraging ICT for Growth, Employment and Governance Project	Leveraging ICT for Growth, Employment and Governance Project	Two (2) weeks from the date of receiving the report
2.1	Technical Cybersecurity Assessment Service Report	(a) Softcopy(PDF) – 1 (b) Hardcopy – 1 (Presentable with excellent feel and look, paper size – A4)	Project Director, Leveraging ICT for Growth, Employment and Governance Project	Leveraging ICT for Growth, Employment and Governance Project	Two (2) weeks from the date of receiving the report
2.2	Information Sharing and Publications Service Report	(a) Softcopy(PDF) – 1 (b) Hardcopy – 1 (Presentable with excellent feel and look, paper size – A4)	Project Director, Leveraging ICT for Growth, Employment and Governance Project	Leveraging ICT for Growth, Employment and Governance Project	Two (2) weeks from the date of receiving the report
2.3	Vulnerability Advisory Service Report	(a) Softcopy(PDF) – 1 (b) Hardcopy – 1 (Presentable with excellent feel and look, paper size – A4)	Project Director, Leveraging ICT for Growth, Employment and Governance Project	Leveraging ICT for Growth, Employment and Governance Project	Two (2) weeks from the date of receiving the report
2.4	Promoting Cybersecurity Service Report	(a) Softcopy(PDF) – 1 (b) Hardcopy – 1 (Presentable with excellent feel and look, paper size – A4)	Project Director, Leveraging ICT for Growth, Employment and Governance Project	Leveraging ICT for Growth, Employment and Governance Project	One (1) from the date of receiving the report
2.5	Enlarging service delivery capacity Report	(a) Softcopy(PDF) – 1 (b) Hardcopy – 1 (Presentable with excellent feel and look, paper size – A4)	Project Director, Leveraging ICT for Growth, Employment and Governance Project	Leveraging ICT for Growth, Employment and Governance Project	Two (2) weeks from the date of receiving the report

SL. #	Report Name	Report Format and Quantity	Submit To	To be reviewed by	Review and Response Time
3.1	Security compliance for new IT systems deployable to NDC Report	(a) Softcopy(PDF) – 1 (b) Hardcopy – 1 (Presentable with excellent feel and look, paper size – A4)	Project Director, Leveraging ICT for Growth, Employment and Governance Project	Leveraging ICT for Growth, Employment and Governance Project	Two (2) weeks from the date of receiving the report
3.2	Manual on cyber security controls for classified information	(a) Softcopy(PDF) – 1 (b) Hardcopy – 1 (Presentable with excellent feel and look, paper size – A4)	Project Director, Leveraging ICT for Growth, Employment and Governance Project	Leveraging ICT for Growth, Employment and Governance Project	Two (2) weeks from the date of receiving the report
4.1	Project Inception Report	Softcopy(PDF) – 1 Hardcopy – 1 (Presentable with excellent feel and look)	Project Director, Leveraging ICT for Growth, Employment and Governance Project	Leveraging ICT for Growth, Employment and Governance Project	Two (2) weeks from the date of receiving the report
4.2	Monthly Project Progress Reports	(a) Softcopy(PDF) – 1 (b) Hardcopy – 1 (Presentable with excellent feel and look, paper size – A4)	Project Director, Leveraging ICT for Growth, Employment and Governance Project	Leveraging ICT for Growth, Employment and Governance Project	Two (2) weeks from the date of receiving the report
4.3	Final Report	(a) Softcopy(PDF) – 1 (b) Hardcopy – 1 (Presentable with excellent feel and look, paper size – A4)	Project Director, Leveraging ICT for Growth, Employment and Governance Project	Leveraging ICT for Growth, Employment and Governance Project	Two (2) weeks from the date of receiving the report
4.4	Summary of the Final Report	(a) Softcopy(PPTX)–1 (b) Hardcopy – 6 (Presentable with excellent feel and look, paper size – A4)	Project Director, Leveraging ICT for Growth, Employment and Governance Project	Leveraging ICT for Growth, Employment and Governance Project	Two (2) weeks from the date of receiving the report

6. Qualification Requirements for the Firm

- The firm should have experience of rolling out (prepare design, doing implementation services, supervising process of becoming part of FIRST.org) CIRTs at the national or governmental level in at least two countries in Asia. The firm must provide documentary evidence of description of contracts and amounts, descriptions of services conducted, reference of person to confirm the experience.
- The firm should have undertaken CIRT establishment or CIRT operations assignments of at least 2 (two) similar projects/assignments, one of them having

contract value of not less than 500 000 US$ in developing countries in the last 5 years.

- The firm should have capability in design, development and delivery of information security policies, standards and guidelines related to the CIRT domain. The firm must provide documentary evidence of description of contracts and amounts, descriptions of services conducted, reference of person to confirm the experience.
- The firm should have strong partnerships within international CSIRT community. The firm must provide documentary evidence of list of strong formal and informal partnerships with and within international CSIRT communities.

7. Consultant Team

7.1. Qualification and Experience of the Key Professional Staff:

We envisage the consultant team providing effort of 3-4 Full Time equivalent (FTEs), with at least 1-2 of the core team members being full-time on this assignment for its duration. The firm needs to demonstrate that the team has the suitable mix of skills and experience to be successful in delivering this assignment, including continuity of project leadership and management, coupled with extremely effective on-the-ground stakeholder engagement and client responsiveness.

The consultant team needs to demonstrate experience in the following areas:

- Significant and recent experience in developing country level cyber security incident response capabilities at mature level.
- Recent experience in engaging with international thought leaders on cutting edge technology and transformation issues related to cyber security and e-Government.
- Technical expertise in a variety of cyber security subject matters, including but not limited to incident response, detection, protection, analysis, forensics, business continuity of government, threat intelligence, data sharing solutions, applications and data standards.
- Knowledge and experience in cyber security with practical experience of advising governments on designing and implementing large scale cyber security initiatives.
- Knowledge and expertise regarding use of cyber-secure ICT in public sector and experience in development, planning and execution of cyber security projects in more than one country.
- Ability to engage with senior political, government and business figures and ability to communicate complex technical matters to non-technical decision makers.
- Relevant experience in development of commercial models and contracts, including PPP contracts, for the supply and sharing of cyber security information.
- Prior experience in a public sector environment in a South Asian country.

The above skills and experience need to be demonstrated by the core members of the consulting team assigned to this project, not simply by the broader experience of the consulting firm as a whole.

1. **Team and project leader**:

- University Bachelor’s degree in computer science, IT, engineering or related field;
- Demonstrated application of international best practices in CIRT maturity establishment for at least 2 (two) organisations;
- Demonstrated application of CIRT technologies and tools available in the market in at least 2 (two) organisations and 5 (five) incident response cases;

- Demonstrated at least 2 (two) years of international experience in transfer of knowledge on cyber security;
- Demonstrated at least 2 (two) years of experience working in South Asia region culture;
- Demonstrated at least 10 (ten) years of experience in managing national/government/industry CIRT(s);
- Demonstrated at least 10 (ten) years of experience in providing incident handling, vulnerability assessment and penetration testing, security consulting and awareness raising services;
- Possession of internationally recognized vulnerability management certification.

2. **CIRT technical implementation lead**:

- University Bachelor's or Master's degree in computer science, IT, engineering or related field;
- Possession of internationally recognized cyber security or system engineering certification;
- Demonstrated practical experience of at least 2 (two) years in automating CIRT/SOC activities and processes;
- Demonstrated application of international best practices in CIRT maturity establishment for at least 2 (two) organisations;
- Demonstrated application of CIRT technologies and tools available in the market in at least 2 (two) organisations and 5 (five) incident response cases;
- Demonstrated at least 5 (five) years of experience in technical leadership role in information/ IT/ cyber security;
- Demonstrated experience in leading the technical establishment of at least one national, government, or sector level CIRT, which is approved as member of FIRST.org;
- Demonstrated at least 2 (two) years of working experience in designing and deploying government, sector, or national cyber security policies.

3. **Security policy expert:**

- University Bachelor's or Master's degree;
- Demonstrated at least 2 (two) experience in information security governance;
- Demonstrated at least 5 (five) years of experience in public sector mandates and processes related to security;
- Demonstrated at least 5 (five) years of experience analysis of state and non-state threats to government or national security;
- Demonstrated at least 5 (five) years of working experience in government agencies with high data sensitivity;
- Demonstrated at least 5 (five) years of experience in information security, IT security or related field;
- Demonstrated experience in setting government or national policies for protection of sensitive/ classified information;
- Demonstrated experience in identification, assessment, forecasting and prevention of threats to government or national security;
- Demonstrated international working experience (at least two projects in two different countries).

4. **Information security expert** –

- University Bachelor's degree in technical discipline, such as computer science or engineering;
- Internationally recognized certification in information security management (from EC-Council, SANS, ISACA or similar organisations);
- Demonstrated experience in applying in projects information security principles, vulnerabilities and risk analysis;
- Demonstrated experience of working with Bangladesh information security stakeholders, regulations and culture;
- Demonstrated at least 5 (five) years of working experience in an IT security management position;
- Demonstrated at least 2 (two) years of working experience in a CIRT/SOC organisations;
- Demonstrated at least 2 (two) years of experience in information security design, administrative, logical and physical controls, cyber security consultancy, framework design, policymaking, project development, etc.;
- Demonstration at least 2 (two) years of applied technical knowledge of major networking systems, platforms, applications, etc.

Non-Key Professional Staff:

In addition to key experts in the opinion of the Consultant, the following non-key experts are required to deliver the service in accordance to TOR. Indicative non-key experts are a guideline for the Consultant. The consultants are free to make their own estimate to propose non-key experts.

1. Cyber security architect
2. Cyber security administrator
3. Cyber security analyst
4. Cyber security consultant
5. Network engineer
6. Public relations officer
7. Systems administrator
8. Systems engineer
9. Lawyer with experience in information security

CVs of the proposed non-key professional staff must be provided.

8. Counterpart facilities

The project will provide institutional support and all available documents, data and information to the Consultant. The Consultant should include all eligible expenditure in the financial proposal for accommodation, logistics and required manpower for successful implementation of the assignment.

9. Local Implementation Partner

In Bangladesh, a Consultant must work in a close partnership with a local company. Local partner must ensure that all local logistics, transport, administrative and legal support is present locally.

10. Duration

The entire consultancy work including submission of reports, documents etc. shall be completed within 15 (Fifteen) months from the commencement date.