International Telecommunication Union

Telecommunication Development Bureau

"ENHANCING CYBERSECURITY IN LEAST DEVELOPED COUNTRIES, INCLUDING CIRT(S) ESTABLISHMENT"

Location(s)	LDCs Countries in the Arab Region
Expected duration	3 years
Estimated Budget	Total: **USD 600,000**
Implementing Agency	International Telecommunication Union (ITU)
Contact Information	Rouda.alamirali@itu.int

Brief Description:

Having been mandated by Resolution 130 and Resolution 69 to ensure safe and secure environment and build confidence in the use of telecommunications and ICTs, and to facilitate creation of national computer incident response teams, particularly for developing countries, and cooperation between them; the ITU will assist Member States from the least developed countries in the Arab region in establishing and further developing their cybersecurity capabilities, including the establishment of their national Computer Incident Response Teams (CIRTs). ITU will assist in building and deploying the technical capabilities and related trainings necessary to establish national CIRTs in the LDCs. Thus, it is expected to lead to the development of cybersecurity capacity in these countries while moving forward on enhancing regional and international collaboration.

1. BACKGROUND AND CONTEXT

Cybersecurity is a paramount for sustaining a technologically sound model. Malicious online agents are numerous, organized and of diverse persuasions: political, criminal, terrorist, hacktivist. The tools at their disposal become more sophisticated and complex over time and with experience; the growing number of connected platforms only serves to offer new attack vectors. The Internet itself has become a critical infrastructure to many nations, businesses and people that must also be protected. In embracing technological progress, cybersecurity must form an integral and indivisible part of that process.

Unfortunately, cybersecurity is not yet at the core of many national and industrial technology strategies. Although cybersecurity efforts are numerous, they are eclectic and dispread. Information sharing and cooperation are key to tackling cross-border threats. Such elements require a certain measure of organization in a multitude of disciplines: legal, technical, educational. While a particular country or a specific sector will have developed and adopted a highly effective cybersecurity framework, the knowledge is rarely shared outside of that circle. It is important for each government to create or identify an organization to serve as a focal point for securing cyberspace and the protection of critical information infrastructure, and whose mission includes watch, warning, response and recovery efforts and the facilitation of collaboration between government entities, the private sector, academia, and the international community[1] when dealing with cybersecurity issues.

During the last World Telecommunication Development Conference (WTDC2014), five regional initiatives were introduced and adopted by Arab countries. The purpose of these regional initiatives is to highlight the countries needs and focus efforts in the region over the course of years (2015-2017) on these priority areas as. One of these initiatives in the Arab region is entitled: “Building confidence and security in the Use of telecommunications/ICTs”. The Output 3.1 of Objective 3 of the Dubai Action Plan is to support the ITU membership, in particular developing countries, in addressing the issues identified by WTDC-14 among others on establishing organizational structures, such as computer incident response teams (CIRTs), to identify, manage and respond to cyberthreats, and participate in cooperation mechanisms at the regional and international level. This proved that there is a high demand in the Arab region for creating a secure environment for the ICTs platforms and services. A skilled and educated workforce will enable the

[1] http://www.itu.int/md/D06-SG01-C-0249/en

region to develop this vibrant knowledge society and use the ICTs as main river for sustainable development. The establishment of a CIRT is needed to help to ensure the protection of a nation's critical information infrastructures, and to assist in drafting the overall plan on a country's approach to cybersecurity related issues, and thus can serve as a focal point for further building and implementing a culture of cybersecurity.

2. Overall Objective

The main objective of the project is to assist the Governments of the LDCs countries in the Arab region in establishing and further developing their cybersecurity capabilities, including the establishment of a Computer Incident Response Teams.

Specific objectives are:

- To facilitate the establishment of watch-warning and incident response capabilities to better identify, respond to, and manage cyber-threats;
- To assist the LDCS Member States in identifying its critical information infrastructure sectors and establishing a foundation to be able to further elaborate and implement a systemic cybersecurity strategy; and
- To build the capacity of and transfer know-how to the LDC Governments that are required in order to facilitate further development within the area of critical information infrastructure protection, such as establishing sector CIRTs, etc.

3. Project Strategy

Based on the above objectives, the project will aim to utilize the regional and ITU resources and facilitate one aspect of the Cyber Security Strategy, that is, the establishment of the CIRTs in Arab LDCs countries. As such, the aim is to initially equip the Government of these countries with functioning CIRTs.

The focus for the Human and Institutional Capacity Building activities that will be implemented under this project will be guided by the regional priorities reflected in the Arab Regional Initiative "Building confidence and security in the Use of telecommunications/ICTs".

The project will build on already ITU existing expertise in these areas and could use the current Arab Regional Cybersecurity Center to implement the related activities within the project.

4. Expected Results

- A functioning CIRTs able to provide constituents in the LDC countries with a basic set of services;
- Enhanced expertise on cybersecurity and reduction of the human capacity gap in cybersecurity;
- Improved preparedness on the identification, prevention, response, and resolution of cybersecurity incidents (preliminary assessment and post implementation assessment required);

- Utilization and operation of the CIRT(s) by building an effective/efficient capable CIRT(s) that is ready to respond to cyber attacks targeting the critical information infrastructure. The CIRT will be the trusted advisor to the Government of the LDC countries on matters concerning cybersecurity ;
- National awareness training programmes are developed to result in improvements in cybersecurity procedures, to defend and protect infrastructures and government agencies; and
- Increased ability to enact effective security measures and instill mature responses when such threats occur.

5. Indicators

- National CIRTs established in 3 LDC countries in the Arab region and put into operation by the end of the project;
- At least three (3) government officials from each beneficiary LDC will be trained to manage the CIRT;
- Drafting of roadmap on the building of a culture of cybersecurity as outlined in the Cyber Security Strategy.

6. Activities

The following key activities will be undertaken:

ITU:

- Prepare terms of reference of the subcontractor and contracting with such subcontractor as per the Agreement.
- Selection of the subcontractor and reward of the contract as per the terms of reference Elaborate technical specifications on the IT infrastructures (hardware & software) to host the CIRT solution
- Procure and ship the recommended equipment (hardware & software) as per the technical specifications
- Provide site assessment and preparation for project start.
- Provide and update project plan and roadmap with feasible dates throughout the project.
- Provide capacity building and training based on gaps in the areas identified by ITU during the project implementation.
- Customize training materials for the purpose of aligning them with the beneficiary Governments' goals on cybersecurity capacity building.
- Train experts – further developing of existing skills available in the country.

- Customize and develop processes to run CIRT operations.
- Customize CIRT software to meet beneficiaries needs and be in line with the relevant processes and strategy.
- Remote installation of CIRT software tools, including the following:
  - A Public Portal
  - Request Tracker for Incident Response (RTIR)
  - Mailing list
- Start the operation and conduct post implementation assessment of the operations/implementation of the CIRT project for Quality Assurance.

Beneficiary Countries:

- Assisting site preparation for CIRT Installation.
- Provide a project team of at least three officials, comprising a CIRT Manager and at least two analysts
- Assisting the project team in terms of logistics for training sessions.
- Preparing, together with the Project team, with the assistance of ITU and the subcontractor, the materials to conduct awareness activities.
- Meeting the back-end requirements of the IT infrastructure that host the Public Portal, RTIR and Mailing List; such as operating system configurations, network configurations, or any other fine tuning related to the availability of these systems or ITU experts, or the intended end users of these systems.
- Oversee the involvement of required entities and be responsible for the promotion of the project among the media and local communities with a view to getting stakeholders' continued involvement and to disseminating knowldege about the project and its importance.

7. Inputs

The project implementation will depend on the successful mobilization of resources (human, material and financial). It is envisaged that the project will require funding to the tune of **USD 600,000**. This amount to be used for CIRTs establishment in identified LDC countries.

Project funding will be raised from private and public sources within the Region, as well as international Funding institutions.

ITU:

IN-KIND CONTRIBUTION: ITU will provide skills, Identifying experts and consultants in the region to work with and care and diligence to ensure the success of the project.

Beneficiary Countries:

1. IN-KIND CONTRIBUTION: Assist in identifying regional location, Human resources to implement and run the entire project (minimum 3 individuals)
2. Facility (physical location & office related infrastructure).

Partners:

Cash CONTRIBUTION: The Partners will provide funding support for the implementation of the project.

8. Risks

The risks include failure to raise the funding resources required to finance this project. This risk could be mitigated by using the ITU wide network of partners through which this project could be sold. ITU also has in-house capabilities for fundraising activities and it is the intention to activate these capabilities for this project.

Furthermore, political instability in the Region may militate against resource mobilization efforts or even implementation. Also, lack of support for the project at national and regional level may hamper the implementation.

9. Sustainability

A human capacity-building component has been incorporated in the project implementation to ensure that adequate regional capabilities will be developed within the region. Furthermore sustainability of the established CIRTs will be guaranteed by the beneficiary Governments, as these Governments should commit itself to take necessary measures in order to keep the national CIRT in their countries in operation.

10. Management

The project will be managed by the ITU Project Manager in close collaboration with country counterparts and partners yet to be identified, as well as representatives from regional organizations and some beneficiary countries.

The ITU shall be the implementing agency, and shall be responsible for the recruitment of project experts including the project manager.

11. Budget

The proposed budget of the project is $ USD **600,000** and this includes expert recruitment's, training materials developments and travel.