International Telecommunication Union
*Telecommunication Development Bureau*

| | |
|---|---|
| Project Budget Number: | |
| Project Title: | NATIONAL CIRT ESTABLISHMENT |
| Project Short Title: | NCIRT <COUNTRY> |
| Start Date: | August 2011 |
| Estimated End Date: | Q1 - 2012 |
| Government Coop. Agency: | <Entity in charge> |
| Beneficiary Country: | <COUNTRY> |
| ITU Project Manager: | Marco Obiso |

**SUMMARY OF CONTRIBUTIONS**

***A) Project Budget***

| **Description** | **CHF** |
|---|---|
| Purchase of Services | |
| Mission | |
| Miscellaneous | |
| Other Charges | |
| Total | |
| AOS (7.5%) on in-cash contribution | |
| **Grand Total:** | |

*Brief Description:*

The main goal of the project is to assist <COUNTRY> to establish its national CIRT (Computer Incident Response Team), to serve as a trusted, central coordination point of contact for cybersecurity, aimed at identifying, defending, responding and managing cyber threats.

ITU will assist <COUNTRY> in building and deploying the technical capabilities and related trainings necessary to establish its national CIRT. Thus it is expected to lead to development of national cybersecurity capacity while moving forward on enhancing regional and international collaboration.

| On Behalf of | Signature | Date | Name/Title |
|---|---|---|---|
| ITU: | | | Mr. Brahima Sanou<br>Director of BDT |

<COUNTRY>:

## 1. Background & Context

### 1.1 General Introduction

Many countries and governments are using the dynamic and inter-connected environment of today's networked information systems to improve communications, provide control, protect information, and encourage competitiveness. Computers have become such an integral part of daily activities that computer-related risks cannot be separated from general business, health, and privacy risks. Valuable country assets and critical national infrastructures are now at risk over the Internet.

Overall reliance on the Internet continues to increase[1]. Unfortunately, in this dynamic, distributed, and interconnected environment cyber attacks occur rapidly and can spread across the globe in minutes without regard to borders, geography, or national jurisdiction. As a result, there is a growing need to be able to communicate, coordinate, analyze, and respond to cyber attacks across different business sectors and national borders. The Internet itself has become a critical infrastructure[2] to many nations, businesses and people that must also be protected.

It is important for governments to create or identify a national organization to serve as a focal point for securing cyberspace and the protection of critical information infrastructure, and whose national mission includes watch, warning, response and recovery efforts and the facilitation of collaboration between government entities, the private sector, academia, and the international community[3] when dealing with cybersecurity issues.

Therefore, collaboration at the national and international level is necessary to effectively align capabilities and expertise to manage incidents and raise awareness of potential incidents and steps toward remediation. Governments have the key role in ensuring coordination among these entities.

The establishment of a national CIRT is needed to help to ensure the protection of the nation's critical information infrastructures, assist in drafting the overall plan on the country's approach to cybersecurity related issues, and thus can serve as a focal point for further building and implementing the national culture of cybersecurity.

### 1.2 Problem Statement

The national CIRT has a key role to play in supporting the Government in addressing cybersecurity related issues at the national level as this pertains to preparing for, detecting, managing, and responding to cyber incidents if and when they occur. However, implementing an incident management mechanism requires consideration for funding, human resources, training, technological capability, government and private sector relationships, and legal requirements[4].

[1] http://www.cert.org/archive/pdf/NationalCSIRTs.pdf
[2] http://www.itu.int/ITU-D/connect/flagship_initiatives/impact.html
[3] http://www.itu.int/md/D06-SG01-C-0249/en
[4] http://www.itu.int/md/D06-SG01-C-0249/en

Taking the foregoing into consideration, developing countries, with limited human, institutional and financial resources face particular challenges in elaborating and implementing national policies and frameworks for cybersecurity and critical information infrastructure protection.

### 1.3 Justification

This project focuses on assisting countries to organize and equip themselves to better respond to cyber-threats. It pays particular attention to improving cybersecurity to ensure better protection of a country's ICT infrastructure, including critical information infrastructure, and the availability of dependent services provided to government agencies, citizens and businesses. Many of these services are part of daily life and have a direct impact on a country's economic well-being and progress.

A national CIRT is a key component of a national approach to cybersecurity and is a solid building block onto which other cybersecurity related activities could be linked. The establishment of a national CIRT, and development of related processes on the national level, can also serve as a foundation for the development of the following activities:

- building a knowledgebase that supports the country's development and implementation of a national cybersecurity strategy as well as a national approach for the protection of critical information infrastructures;
- supporting the building of a national culture of cybersecurity, and related awareness raising initiatives;
- supporting the development of related national cybersecurity platforms, for example: the national PKI, e-Government framework and approach, national identity and access management framework, combating SPAM, botnets, etc;
- assisting in planning/development of a national strategy on child online protection;
- further enabling the country to develop and enhance its national incident response and management capabilities.

### 1.4 Relationship to BDT Programs/Activities

The objective of Programme 2 of the Hyderabad Action Plan is to support the ITU membership, in particular developing countries, in addressing the issues identified by WTDC-10 among others on *establishing organizational structures, such as computer incident response teams (CIRTs), to identify, manage and respond to cyberthreats, and cooperation mechanisms at the regional and international level.*

For this reason, Resolution 69 *"Creation of national computer incident response teams, particularly for developing countries, and cooperation between them*" was adopted at WTDC-10.

As lead facilitator for WSIS Action Line C5[5], ITU is responsible for assisting stakeholders in building confidence and security in the use of Information and Communication Technologies (ICTs)[6] at national, regional and international levels.

ITU Resolution 130 (Guadalajara, 2010) on "Strengthening the role of ITU in building confidence and security in the use of information and communication technologies"; **in particular *instructs the Director of the Telecommunication Development Bureau***

- *to develop, consistent with the results of WTDC-10 and pursuant to **Resolution 45 (Rev. Hyderabad, 2010), Resolution 69 (Hyderabad, 2010)** and Programme 2 in the Hyderabad Action Plan, the project for enhancing cooperation on cybersecurity and combating spam in response to the needs of developing countries, in close collaboration with the relevant partners;*
- *upon request, to support ITU Member States in their efforts to build capacity, by facilitating Member States' access to resources developed by other relevant international organizations that are working on national legislation to combat cybercrime; supporting ITU Member States' national and regional efforts to build capacity to protect against cyberthreats/cybercrime, in collaboration with one another; consistent with the national legislation of Member States referred to above, assisting Member States, in particular developing countries, in the elaboration of appropriate and workable legal measures relating to protection against cyberthreats at national, regional and international levels; establishing technical and procedural measures, aimed at securing national ICT infrastructures, taking into the account the work of the relevant ITU-T study groups and, as appropriate, other relevant organizations**; establishing organizational structures, such as CIRTs, to identify, manage and respond to cyberthreats, and cooperation mechanisms at the regional and international level;***
- *to provide the necessary financial and administrative support for this project within existing resources, and to seek additional resources (in cash and in kind) for the implementation of this project through partnership agreements;*
- *to coordinate the work of this project with that of the ITU-D study groups on this topic, and with the relevant programme activities and the General Secretariat;*
- *to continue collaboration with relevant organizations with a view to exchanging best practices and disseminating information through, for example, joint workshops and training sessions;*
- ***further instructs the Director of the Telecommunication Standardization Bureau and the Director of the Telecommunication Development Bureau,*** each within the scope of his responsibilities:

[5] http://www.itu.int/osg/csd/cybersecurity/WSIS/
[6] http://www.itu.int/wsis/docs/geneva/official/poa.html

- to implement relevant resolutions of both WTSA-08 and WTDC-10, including Programme 2 on providing support and assistance to developing countries in building confidence and security in the use of ICTs;
- to identify and promote the availability of information on building confidence and security in the use of ICTs, specifically related to the ICT infrastructure, for Member States, Sector Members and relevant organizations;
- without duplicating the work under ITU-D Question 22-1/1, to identify best practices in establishing CIRTs, to prepare a reference guide for the Member States and, where appropriate, to contribute to Question 22-1/1;
- to cooperate with relevant organizations and other relevant international and national experts, as appropriate, in order to identify best practices in the establishment of CIRTs;
- to take action with a view to new Questions being examined by the study groups within the Sectors on the establishment of confidence and security in the use of ICT;
- to support strategy, organization, awareness-raising, cooperation, evaluation and skills development;
- to provide the necessary technical and financial support, within the constraints of existing budgetary resources, in accordance with Resolution 58 (Johannesburg, 2008);
- to mobilize appropriate extrabudgetary resources, outside the regular budget of the Union, for the implementation of this resolution, to help developing countries;
- ITU-D Study Group 1, Question 22 activity for the development of a report on: "Best Practices For A National Approach To Cybersecurity: Building Blocks For Organizing National Cybersecurity Efforts".

WTDC-10 calls on assisting Member States in establishing organizational structures, such as CIRTs, to identify, manage and respond to cyberthreats, and cooperation mechanisms at the regional and international level.

In this framework, the Global Cybersecurity Agenda (GCA) was launched by the ITU Secretary-General as ITU's framework for international multi-stakeholder cooperation towards a safer and more secure information society, and focuses on the following five work areas:

- Legal Measures
- Technical and Procedural Measures
- Organizational Structures
- Capacity Building
- International Cooperation

Within the GCA's framework and as part of efforts to achieve global coordination and international cooperation on cybersecurity, ITU, in September 2008, signed a Memorandum of Understanding with the International Multilateral Partnership against Cyber-Threats (IMPACT).

## 2. Strategy

### 2.1 Overall Project Objective

The objective of this project is to assist <COUNTRY> in establishing and further developing its cybersecurity capabilities, including the establishment of a Computer Incident Response Team with national responsibility.

### 2.2 Project Strategy

The overall strategy is to facilitate the process towards the establishment of a global cybersecurity strategy for each of the involved Member States. As such the aim is to initially equip Member States with functioning CIRTs, to be extended to other interested Member States in the future.
This project will:

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

## 3. Outputs

By implementing this project, the following primary and secondary outcomes are expected:

### 3.1 Primary Output:

- A functioning national CIRT able to provide its constituents with a basic set of services.

### 3.2 Secondary Outputs:

- Enhanced national expertise on cybersecurity and reduction of the human capacity gap in cybersecurity.

- Improved national preparedness on the identification, prevention, response, and resolution of cybersecurity incidents (preliminary assessment and post implementation assessment required).
- Utilization and operation of the CIRT by building an effective/efficient capable CIRT that is ready to respond to cyber attacks targeting the national critical information infrastructure. The national CIRT will be the trusted advisor to the government 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.
- Increased ability to enact effective security measures and instill mature responses when such true threats occur.

## 4. Indicators

Indicators are:

- National CIRT established and put into operation by the end of the project;
- at least three (3) government officials from <COUNTRY> will be trained to manage the national CIRT;
- Drafting of roadmap on the building of a national culture of cybersecurity as a part of national cybersecurity strategy within the framework of national CIRT enhancements.

## 5. Activities

To meet the objectives of this project, a number of activities will be undertaken by **the Parties,** as presented below:

### 5.1 ITU Activities

The project activities undertaken will be in synergy with Programme 2 of the Hyderabad Action Plan and ITU planned regional activities, to ensure effective implementation of the project.

ITU specific activities for the project will be to:

- Prepare terms of reference of the subcontractor and contracting with the latter as per the Administrative Agreement.
- 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 during the project implementation.
- Customize training materials that meet <COUNTRY>'s 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 <COUNTRY>'s needs and be in line with the relevant processes and strategy.
- Install CIRT software tools – all activities involved in software installation.
- Start the operation and conduct an assessment of the operations/implementation of the CIRT project for Quality Assurance.
- Prepare together with the <COUNTRY>'s team the awareness creation materials to conduct national activities on awareness rising.

### 5.2 Beneficiary Country Activities

Member State specific project activities will be to:

- Sign the Administrative Agreement with ITU.
- Transfer the allocated funds to ITU.
- Provide physical access to the CIRT facility allocated and provide network access.
- Purchase the recommended equipment - hardware/basic OS software configuration for the CIRT solution deployment.
- Provide project facilities and resources where the project office can be located and training sessions can be conducted.

## 6. Inputs

### 6.1 ITU:

| | |
|---|---|
| IN KIND CONTRIBUTION | HUMAN RESOURCES AND SKILLS FOR PROJECT COORDINATION AND MANAGEMENT - ITU WILL PROVIDE SKILLS, CARE AND DILIGENCE TO ENSURE THE SUCCESS OF THE PROJECT |

### 6.2 <COUNTRY>:

| | |
|---|---|
| IN CASH CONTRIBUTION | |
| IN KIND CONTRIBUTION | 1. FINANCIAL COMMITMENT ON CIRT ESTABLISHMENT & SUSTAINABILITY<br>2. HUMAN RESOURCES TO IMPLEMENT AND RUN THE ENTIRE PROJECT (MIN 3 RESOURCES)<br>3. FACILITY (PHYSICAL LOCATION & RELATED INFRASTRUCTURE)<br>4. HARDWARE AND BASIC SOFTWARE (SERVERS, CLIENTS, OPERATING SYSTEM, NETWORK, ETC.) – ESTIMATE COSTS IN THE ANNEX OF THIS DOCUMENT AT IN-KIND CONTRIBUTION SECTION. |

<COUNTRY> will provide a project team comprising of its own staff (minimum three (3) officials) to implement and coordinate the project on-site with ITU; mobilize local partners; host project team meetings; train the trainers, comprising CIRT manager and analysts; provide local logistics including deployment of equipment and human resources; Internet connection, computer hardware, promote the project among stakeholders in the governmental agencies, etc.

<COUNTRY> will oversee the involvement of required national entities and be responsible for the promotion of the project among the national media and local communities with a view to getting stakeholders' continued involvement and knowledge about the project and its importance. The stakeholders' involvement plays a key role in the overall success and effectiveness of the project.

## 7. Risk Management

- The primary risk for this project is that in-country activities may suffer delays due to unforeseen local events and circumstances. Getting the commitment from the government in early stages of planning will minimize this risk of failure.
- Another factor of risk for the project is the possibility of inadequate human resources assigned to the project (by <COUNTRY>), which would increase the time for completion. This risk will be reduced by provision of appropriate site and country training courses by ITU.
- As a first step, BDT has conducted a feasibility assessment in advance for <COUNTRY> on CIRT Establishment to further manage risks of possible project delay or additional costs.

## 8. Project management

The project will be implemented by the assigned ITU Project Manager in close coordination with <COUNTRY>'s Focal Point(s) and Subcontractor.

ITU as the implementing agency will supervise and administer overall implementation of the project in accordance with ITU rules and procedures.

## 9. Roles and Responsibilities

### 9.1 International Telecommunication Union (ITU)

**ITU will:**

- Provide staff resources for the coordination and management of the project and be responsible for the overall management of the project implementation, supervision, monitoring, coordination and evaluation.
- Provide its expertise and international experience to enable realization of the project objectives in an effective and efficient manner.

- Allocate the experts for the project as per contract and terms of reference.
- Correspond with the relevant parties to make sure that project is successful.
- Provide advice and assistance to the project team, when it is required pre-, during and after project implementation.
- Provide the solution/software source code and related development documentation to the country at no additional charge as a part of the project.
- Identify country's needs and assist in the development of a roadmap for National CIRT evolution.
- Provide a roadmap for human capacity building and training needs for the development of the National CIRT services.
- Transfer the know-how to <COUNTRY> on CIRT and cybersecurity defense against attacks on national critical information infrastructure.
- Produce periodic project progress reports.
- Produce project closure report with financial statement at the completion of the project.

### 9.2 Beneficiary Country

**<COUNTRY> will:**

- Designate national counterparts (qualified technical personnel) that will assist in hosting project team, provide local logistics including deployment of equipment. The national counterparts designated by <COUNTRY> will, in particular, assist ITU and the selected subcontractor by providing accurate information relevant to the project.
- Provide information required for carrying out the planned and agreed project activities.
- Provide human resources to efficiently operate the CIRT.
- Provide physical space, hardware and software facilities as properly required by the project nature and for the establishment of the CIRT.
- Provide administrative support required (including with a view to issuing and delivering visas to the members of the project team and facilitating customs clearance of any necessary equipment, materials, etc.,) required during the project implementation and any other assistance that may be required for the successful project implementation.
- Collect cyber-attacks data, outline statistical trends, attack patterns, build intelligence on top of them and reach effective knowledge sharing.
- Commit necessary resources to keep the national CIRT facilities in operation after completion of the project.

## 10. Project's sustainability

Cyberthreats are increasingly affecting the daily lives of ICT users therefore the national CIRT is considered to be a sustainable solution due to its capabilities against cyberthreats. Furthermore sustainability of the established NCIRT will be guaranteed by <COUNTRY>. As described in section 9 of this project document, <COUNTRY> commits itself to take necessary measures in order to keep the NCIRT in operation.

## 11. Monitoring and evaluation

The Project Manager will prepare periodic progress reports, which will provide a summary of the achiements and activities as well as challenges faced in a given period.

ITU together with <COUNTRY> will, at the end of the project, prepare a final report to assess the success of the project in terms of meeting its stated main objectives, expected outcomes and impacts on the beneficiary country's future development.

For the evaluation of the project, post-implementation feedback from each CIRT country could be requested in order to provide useful lessons in planning and replicating similar implementation projects in future and customization of the training materials.

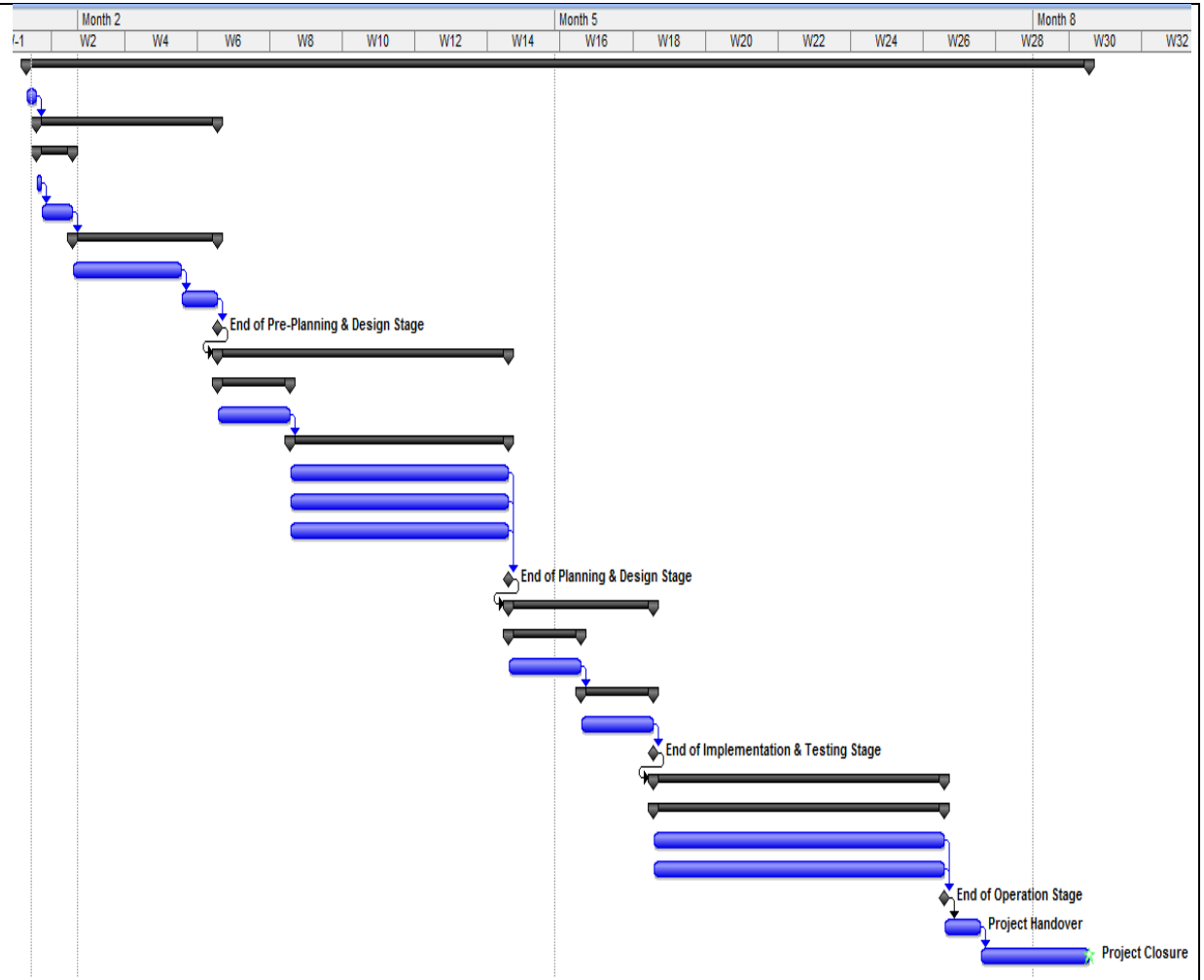
## 12. Work Plan

The work plan is contained in Annex B.

**Annex B.**
**Work plan**

| | Task Name | Duration |
|---|---|---|
| 1 | **National CIRT Establishment** | **147 days** |
| 2 | Onsite Project Kick-off Meeting | 2 days |
| 3 | **Pre-Planning & Design Stage** | **25 days** |
| 4 | **Onsite** | **5 days** |
| 5 | CIRT Awareness Workshop | 1 day |
| 6 | CIRT Implementation Requirements Workshop | 4 days |
| 7 | **Offsite** | **20 days** |
| 8 | Pre-CIRT Implementation Plan | 3 wks |
| 9 | Submit and Review Pre-CIRT Implementation Plan | 1 wk |
| 10 | End of Pre-Planning & Design Stage | 0 days |
| 11 | **Planning & Design Stage** | **40 days** |
| 12 | **Onsite** | **10 days** |
| 13 | Create & Approve User Requirement Specification (URS) | 2 wks |
| 14 | **Offsite** | **30 days** |
| 15 | Design CIRT According to URS | 6 wks |
| 16 | Network Design according to URS | 6 wks |
| 17 | Pre-Installation & Preperation Step by Step Guide for Network & Hardware | 6 wks |
| 18 | End of Planning & Design Stage | 0 days |
| 19 | **Implementation & Testing Stage** | **20 days** |
| 20 | **Offsite** | **10 days** |
| 21 | Remote Installation & Testing | 2 wks |
| 22 | **Onsite** | **10 days** |
| 23 | Fine-tuning of CIRT Application & Training | 2 wks |
| 24 | End of Implementation & Testing Stage | 0 days |
| 25 | **Operation Stage** | **40 days** |
| 26 | **Offsite** | **40 days** |
| 27 | Service Desk Support for CIRT Operations | 8 wks |
| 28 | Final Project Handover Documentation Preparation | 8 wks |
| 29 | End of Operation Stage | 0 days |
| 30 | Project Handover | 1 wk |
| 31 | Project Closure | 3 wks |

Gantt Chart



# CIRT Methodology Overview

| Assessment | Planning & Design | Implementation | Operations | Collaboration |
|---|---|---|---|---|
| • Current State Assessment (questionnaires)<br>• Obtain Management Support and Buy-In through Trusted Communications | • Determine & Confirm Constituency<br>• Define & Confirm Mission Statement<br>• Determine CIRT Services | People:<br>• Trainings | • Incident Handling Activities<br>• Information Dissemination | • Cooperation Between Other CIRTS |
| • Capacity Building through Awareness and Training on the need to establish a National CIRT<br>• Recommendation Report | • Determine ReportingStructure, Authority &Organisation Model<br>• Define CIRT Processes & Workflow<br>• Develop Policies, Procedures and Documentations | Process:<br>• Finalised CIRT Processes & Workflow<br>• Finalised Policies, Procedures&Documentations | • Managing CIRT Staff<br>• Managing CIRT Infrastructure<br>• Identify CIRT Media Spokesperson(s) | |
| | • Identify Interactions with Key Parts of the Constituency<br>• Define Roles and Responsibilities for Interactions<br>• Determine Technology Requirements (HW, SW, Tools, etc.) | Technology:<br>• Assess Infrastructure for theConstituency<br>• Hardware & Software Installation | • Disaster Recovery Plan<br>• Quality Assurance Review | |
| | • Human Resource Requirements<br>• Capacity Building<br>• Communications Approach<br>• CIRT Facilities | Others:<br>• Legal Issues<br>• CIRT Announcement | | |