

# AMERICAS

## **ITU-IMPACT CIRT Assessment in Santo Domingo, Dominican Republic, April 2012**

ITU-IMPACT Alliance conducted a CIRT readiness assessment and capacity building program for Dominican Republic, Ecuador and Honduras at Santo Domingo, Dominican Republic in April 2012.

The missions were aimed at assisting the country in assessing its readiness to implement a national CIRT – a national CIRT will provide the capability to identify, respond and manage cyber threats as well as to enhance the Cybersecurity posture of the country.

The primary objectives of this project are to assist the identified countries in the assessment of its readiness to implement a National CIRT (Computer Incident Response Team) and fulfil all the descriptions of duties as stipulated in the Project Scope below.

The scope of the assessment consists of:

- a) Study and analyze the countries' current Cybersecurity status and needs.
- b) Provide high-level recommendations to improve the Cybersecurity posture of the countries.
- c) Study and suggest institutional and organizational requirements, and arrangements for setting-up National CIRTs.
- d) Capacity building program for the CIRTs.
- e) Conduct trainings for human capacity building to impart knowledge and skills for operation, maintenance and coordination of CIRTs with relevant agencies, both local and international.
- f) Design specifications for hardware and software for the CIRTs.
- g) Include all the above mentioned details with a Mission Report and any other information deemed necessary in a report to be submitted in electronic copy to ITU.

Based on the assessment carried out, it is recommended that the governments of identified countries should focus on setting up national CIRT, which must be appropriately positioned within the government institutional and organisational structure, as soon as possible.

## **ITU-IMPACT CIRT Assessment in St. Georges, Grenada, August 2012**

ITU-IMPACT Alliance conducted a CIRT readiness assessment and capacity building program for Barbados, Grenada, Saint Kitts and Nevis, Saint Vincent and the Grenadines, and Trinidad and Tobago at St. Georges, Grenada in August 2012.

The missions were aimed at assisting the country in assessing its readiness to implement a national CIRT – a national CIRT will provide the capability to identify, respond and manage cyber threats as well as to enhance the Cybersecurity posture of the country.

The primary objectives of this project are to assist the identified countries in the assessment of its readiness to implement a National CIRT (Computer Incident Response Team) and fulfil all the descriptions of duties as stipulated in the Project Scope below.

The scope of the assessment consists of:

- a) Study and analyze the countries' current Cybersecurity status and needs.
- b) Provide high-level recommendations to improve the Cybersecurity posture of the countries.
- c) Study and suggest institutional and organizational requirements, and arrangements for setting-up National CIRTs.
- d) Capacity building program for the CIRTs.
- e) Conduct trainings for human capacity building to impart knowledge and skills for operation, maintenance and coordination of CIRTs with relevant agencies, both local and international.
- f) Design specifications for hardware and software for the CIRTs.
- g) Include all the above mentioned details with a Mission Report and any other information deemed necessary in a report to be submitted in electronic copy to ITU.

Based on the assessment carried out, it is recommended that the governments of the identified countries should focus on setting up national CIRT, which must be appropriately positioned within the government institutional and organisational structure, as soon as possible.