Telecommunication
Development Bureau (BDT)

Ref.: BDT/POL/CYB/Cirular- 002

Geneva, 15 February 2011

Contact: Souheil Marine
Telephone: +41 22 730 6057
Telefax: +41 22 733 5484
E-mail: cybersecurity@itu.int

Member States

Subject: ITU–IMPACT – Deployment of Cybersecurity Capabilities

Dear Madam/Sir,

As new Director of the ITU Telecommunication Development Bureau (BDT), I am writing to inform your Administration that BDT will continue to support the International Multilateral Partnership Against Cyber Threats (IMPACT) and is committed to continuing to assist Member States in building confidence and security in the use of ICTs.

As you know, ITU and IMPACT formally entered into a Memorandum of Understanding in 2008 in which IMPACT's new state-of-the-art global headquarters in Cyberjaya, Malaysia is the physical home and operational arm of the ITU's Global Cybersecurity Agenda (GCA).

The close synergies between the five pillars of the GCA and the service offerings provided by IMPACT made this joint partnership a crucial step in the global fight against cyberthreats and other misuses of ICTs while assisting Member States in building their cybersecurity capabilities.

As BDT Director, I am committed to building upon past successes and implementing new initiatives and projects in response to WTDC-10 and PP-10 resolutions.

ITU, through its Sectors, in particular BDT, has gained significant experience in facilitating the establishment of national strategies for cybersecurity and critical information infrastructure protection, and can draw upon an extensive network of leading cybersecurity authorities and individuals.

In order to properly address the five pillars of the GCA, as well as to follow up on ITU's work to assist countries in developing cybersecurity capabilities, ITU–IMPACT is making available its expertise to allow Member States to detect, analyse and respond to cyberthreats.

The Global Response Center (GRC) has been identified as a global-level platform for early warning system and the foremost cyber threat resource centre for the global community, providing emergency response services and knowledge-sharing mechanisms in a trusted environment.

An integral part of the GRC-related services that ITU–IMPACT is providing to Member States is the Electronically Secure Collaborative Application Platform for Experts (ESCAPE). ESCAPE is a tool which allows cybersecurity experts from different countries to pool their resources, share their expertise and remotely collaborate in a secure environment. The ESCAPE platform enables the GRC to act as a one-stop coordination and response centre for countries in times of crisis, enabling the swift identification and sharing of available resources, as well as incident management and response tools. Some 70 Member States are currently part of the ITU–IMPACT and are benefiting from the GRC, provided free of charge.

Additionally, Member States that join the ITU-IMPACT alliance get access to apply for training and educational scholarships provided by IMPACT and partners such as SANS Institute, EC Council, ISC^2 etc.

Moreover, dedicated organizational structures at a national level need to be established to manage cyber attacks. In this perspective, ITU-IMPACT has elaborated a strategy for the implementation of national Computer Incidents Response Teams (CIRTs), as a trusted, central coordination cybersecurity point of contact within a country, providing watch and warning systems and incident response services. The proposed solution would be integrated into the GRC, already provided to the countries, and would be compliant with international best practices.

ITU-IMPACT has already completed assessments for 21 countries and is planning to continue this effort, moving forward in facilitating the physical implementation of CIRTs, providing the required expertise in recommending the most suitable hardware and software, assisting in elaborating the necessary processes and in building human capacity.

The annexes to this letter provide an overview of the services currently delivered, as well as the necessary documentation to join ITU-IMPACT (sample response letter and country profile to be completed). Additional information on IMPACT can also be found online at:

- http://www.itu.int/ITU-D/cyb/cybersecurity/impact.html

If your country has not already joined the ITU-IMPACT alliance, and would wish to get involved in the activities mentioned above, please respond to this letter, highlighting the specific area and services which are of interest to your country.

I welcome you to the coalition and look forward to your valuable inputs on how to better assist ITU Member States.

Yours faithfully,

Brahima Sanou
Director

Annexes:

- Technical Notes :
  - Global Response Center (GRC)
  - IMPACT Centre for Training and Skill Development
- Sample Response Letter
- Country Profile Form

CC:

- Heads, ITU Regional Offices