



**Telecommunication
Development Bureau (BDT)**

Ref.: BDT/POL/CYB/Circular-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, ISC² 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

Technical Note

I GLOBAL RESPONSE CENTRE (GRC)

INTRODUCTION

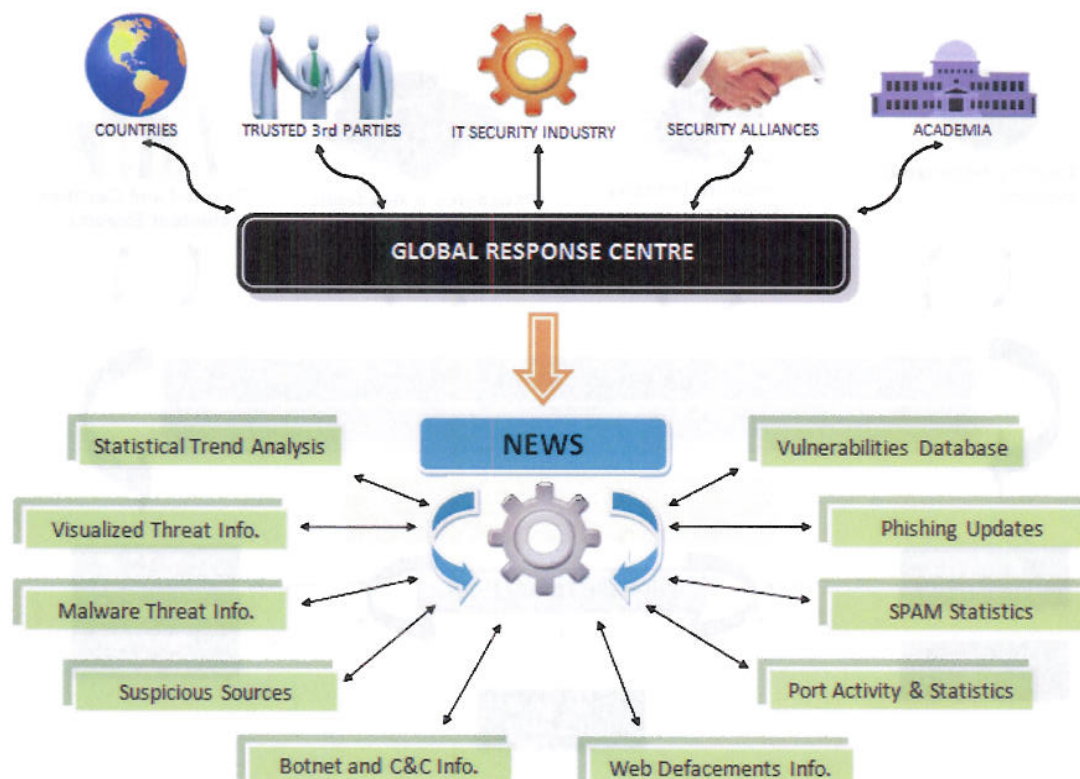
GRC, as one of the key divisions of IMPACT, has evolved as the centralised threat coordination and analysis centre in collaboration with its research and operational partners. Through its extensive partnership with leading vendors from cybersecurity, academic research networks and governments, GRC provides the global community (especially the government sector) with visualisation of emerging threats, near real-time aggregated threat information and a collaboration platform for helping governments to mitigate threats through effective collaboration.

The GRC consists of the two main components offered to the ITU-IMPACT alliance members:

- 1 Network Early Warning System (NEWS) and
- 2 Electronically Secure Collaborative Application Platform for Experts (ESCAPE).

NEWS (Network Early Warning System)

GRC, through its alliances with partners like Microsoft, Symantec, Kaspersky, Trend Micro, ISC², SANS, F-Secure and many more, provides a well developed threat analysis, diagnosis and prioritisation scheme via NEWS. NEWS fuses data from multiple trusted sources and this aggregated data is then made available to key focal points in partner countries. This process provides the ability to rapidly distribute actionable information back to key national agencies, law enforcement agencies and trusted cybersecurity experts who can identify cyber threats at their inception and take necessary measures to prevent them.

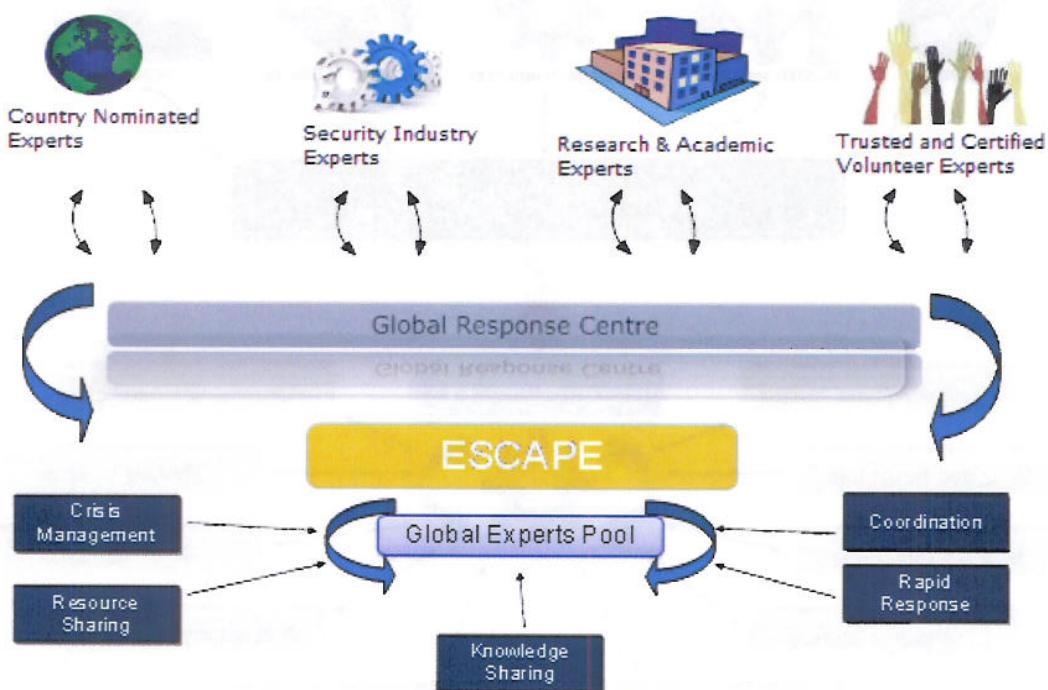


Under this system GRC provides information on different aspects of cybersecurity such as:

- **Malware:** recent malware discovered by vendors across the globe, the details and remediation steps.
- **Suspicious Source IP's:** list of suspicious source IP addresses that the community needs to be aware of, their origin and statistical information.
- **Botnet:** comprehensive information of botnet activities, such as where and how many C&C servers and bots are running. Details of suspicious botnet IP's are also provided.
- **Spam Sources:** aggregated information on spam source addresses and locations.
- **Ports:** that represent higher rates of involvement in suspicious activities from the attacker's side or the target end.
- **Latest Vulnerabilities:** discovered by vendors and other cybersecurity experts that need immediate attention and/or resolution.
- **Phishing:** detailed analysis and other valuable information on phished sites, domains, contents etc to stop further attacks.
- **Web defacements:** on the web page defacements that take place on a daily basis in the world.

ESCAPE (Electronically Secure Collaborative Application Platform For Experts)

ESCAPE is a collaboration platform that enables authorised cyber experts across different countries to collaborate with each other remotely, within a secure environment. This includes IT experts, regulators, Computer Incident Response Teams (CIRTs) and others. It consists of modules such as the Knowledge Exchange Network (KEN), Automated Threat Analysis System (ATAS), Incident Management, Blogs, Forums, security advisories etc. By converging resources and expertise from many different countries at any time, ESCAPE enables partner countries and the global community to collectively respond to cyber threats, especially during crisis or outbreaks.



These systems enable the GRC to act as a one-stop coordination and response centre for partner countries during emergencies, enabling swift identification and the sharing of available resources across borders.

Introductory Package

All member countries are provided access to the GRC’s introductory package. This entitles them to have access to NEWS and ESCAPE. IMPACT’s NEWS provides IMPACT members an up to the minute view of cyber threats around the world. These threats are drawn on data from dozens of public and private security feeds and are presented as a collection of easy to read charts, graphs, maps and tables. NEWS allows the members to seek the sources of attacks emerging round the globe; identify the current cyber threats and cyber security breakouts.

The introductory package also provides the member countries the ability to discover and connect with other cyber security professionals throughout the IMPACT network via ESCAPE. By applying enterprise social networking techniques to IMPACT member countries, IMPACT allows members to draw on the wealth of expertise within the IMPACT community. The introductory package provides up to five multiple logins to the ESCAPE and ability to add local cyber security experts to the IMPACT expert community. With this package the member countries can escalate their security problems to the global IMPACT experts, who provide assistance and right solutions. Furthermore, ESCAPE provides periodic security news, reports, and ability to upload a malware for inspection and analysis by the IMPACT experts.

For the introductory package IMPACT dedicates a Computer Security Incident response team member to provide assistance as and when required.

IMPACT – Introductory Package Functionality Offered

Description	Introductory
Global Response Centre	
• Access to the GRC	From up to 2 Public IP Addresses
• Ability to have access to NEWS data and visualization	√
• Maximum number of NEWS/ESCAPE portal accounts	5
• Ability to invite local experts to the IMPACT expert community	√
• Ability to escalate incidents to the IMPACT expert community	√
• Ability to upload malware for IMPACT analysis	√
• Ability to receive periodic security news	√
• Ability to receive periodic security reports (Generic)	√
• Ability to subscribe to ESCAPE's content	√
• Minimum number of Computer Security Incident Response Team members nominated	3
Training & Skill Development	
• Training on ESCAPE	√
• Training on NEWS	√

Technical Note

II

IMPACT CENTRE FOR TRAINING AND SKILLS DEVELOPMENT

As a global, non-profit organisation, IMPACT has received generous grants from leading information security training providers. These grants enable IMPACT to offer highly sought-after training courses to qualified security professionals from any one of our partner countries. Through this programme, IMPACT is able to offer various training courses courtesy of the SANS Institute and EC-Council. These organisations are widely acknowledged as the top information security certification bodies in the world and are renowned for providing exceptional high quality courses and certifications that are recognised throughout the information security community.



IMPACT-SANS Joint Programme for Improving Cyber-Security Education (ICE)

Scholarship Programme

IMPACT-SANS has jointly partnered to draw out the ICE program with the objective of creating skilled security personnel in both areas of network and application for governments around the world. This ICE program is fully sponsored by IMPACT-SANS and is open to all partner countries of IMPACT – specifically developing nations that have joined IMPACT’s global agenda to address cyber-threats.

SANS security training courses will be awarded to recipients from IMPACT partner countries with the prerequisite background in security. The courses offered are aimed at developing local talents within the partner countries to instructor status, and with the knowledge obtained, the local instructors will be expected to contribute by conducting security seminars, workshops and community programs.

Prospective candidates from IMPACT partner countries are required to fill out an application form, inclusive of a letter of support from their local government representative, before being screened for eligibility. It is hoped that the awareness, training and education program provided through ICE will benefit IMPACT partner countries and at the same time, contribute to enhance cyber-space security for all.



IMPACT-EC-Council Training Scholarship Programme

IMPACT- EC-Council is offering an exclusive scholarship program to assist partner countries of IMPACT to develop more skilled, knowledgeable and certified information security professionals and practitioners. This programme is specifically designed to assist governments, businesses and academia to raise their capability and competency, to combat cyber threats and to remain resilient.

IMPACT-EC-Council provides full scholarship to qualified candidates to attend the following web-based courses:

- Network Security Administrator (**E|NSA**)
- Certified Ethical Hacker (**C|EH**)
- Computer Hacking Forensic Investigator (**C|HFI**)
- Certified Security Analyst (**E|CSA**)
- Licensed Penetration Tester (**L|PT**)
- Certified Disaster Recovery Professional (**E|DRP**)

IMPACT Training and Skills Development Programmes

IMPACT offers a full range of structured and specialised training courses that to partner countries and organisations. These courses are conducted by world class instructors with proven expertise in their particular disciplines. All IMPACT courses are designed, developed and delivered to provide clients with the necessary skills and knowledge required to understand the technologies involved and key security mission they are addressing. Due to the complexity and rapid advancement of technology, it is vital to establish high standards for development of these courses.

We believe in developing courses to enhance the knowledge and skills of IT Security developers and professionals. This would enable businesses and organisations to heighten their capabilities in managing and securing their IT infrastructures, business processes and most importantly, the people themselves. Our challenge is to ensure the knowledge and skills gained from a course are current, relevant and applicable to their job function as a security professional.

The key to success in the field of information security is to begin with a course that gives in-depth foundation in the vital areas of information security, with a view to specialised areas of cybersecurity, relevant to an individual's job function. The **IMPACT SecurityCore**, developed by IMPACT, is a prerequisite that leads to the two specialised areas of cybersecurity - **Technical** and **Management**. The participants are able to escalate their knowledge and skills by attending the specialised courses under these tracks. Other courses offered by this centre include Network Forensics and Investigation, Malware Analysis and Reverse Engineering, Securing ISP Networks & Systems and Network Investigation for Law Enforcement.

Sample Response Letter

Mr. Brahim Sanou
Director
Telecommunication Development Bureau
International Telecommunication Union
Place des Nations
CH-1211 Geneva 20
Switzerland

Ref : BDT/POL/CYB Circular-002

Subject: Deployment of Cybersecurity capabilities - IMPACT Global Response Center

Dear Director,

In reference to your letter on the aforementioned subject, we would like to thank you for the opportunity given to <COUNTRY> to be involved in the ITU-IMPACT initiative.

In this regard, we are pleased to confirm our interest in joining the coalition and have the opportunity to receive concrete services and facilities within the framework of the ITU Global Cybersecurity Agenda and support the ITU Development Sector in its efforts toward achieving Cybersecurity.

In consideration for <COUNTRY> being a Partner and obtaining access to the services of the GRC and the facilities of IMPACT, <COUNTRY> is interested in the following areas:

Global Response Center (NEWS,ESCAPE)
Training and skills development
Centre for Security Assurance and Research
Centre for Policy and International Cooperation

Thank you and looking forward for our future fruitful collaboration and cooperation.

Yours sincerely,

Date

Country Profile Form

IMPACT COUNTRY PROFILE

1. COUNTRY DETAILS:

Country	<input type="text"/>	Currency	<input type="text"/>
Capital	<input type="text"/>	Timezone	<input type="text"/>
Country Code (dialling in)	<input type="text"/>	International Prefix (dialling out)	<input type="text"/>
Mobile Technology	<input type="text"/>	Neighbouring Countries	<input type="text"/>
International Memberships	<input type="text"/>		

2. COUNTRY CYBERSECURITY FOCAL POINT:

Name	<input type="text"/>		
Address	<input type="text"/>		
City	<input type="text"/>	State	<input type="text"/>
	Zip Code	<input type="text"/>	
Website	<input type="text"/>		
Phone	<input type="text"/>	Fax	<input type="text"/>

Main Contacts:

Name	Position	Telephone	Email

Year Created Number of Staff

Reports To

Responsibilities:

<input type="checkbox"/> ISP Licencing	<input type="checkbox"/> Cybersecurity Law Maker
<input type="checkbox"/> Spectrum Management	<input type="checkbox"/> Quality Monitoring
<input type="checkbox"/> Certification & Certifying	<input type="checkbox"/> Economic Regulation
<input type="checkbox"/> Dispute Resolution	<input type="checkbox"/> Technical Regulation
<input type="checkbox"/> Universal Service Provision	<input type="checkbox"/> Mandatory Standards
<input type="checkbox"/> Rate Regulation & Monitoring	<input type="checkbox"/> Information Security
<input type="checkbox"/> Enforcement	<input type="checkbox"/> Technology Roadmap
<input type="checkbox"/> Others:	<input type="text"/>

3. COMPUTER INCIDENT RESPONSE TEAM INFORMATION (If Present):

Organization

Address

City State Zip Code

Website

Main Contact Phone

Email Fax

4. COUNTRY'S LAWS & LEGISLATIONS ON CYBERSECURITY:

(Briefly explain the adoption of appropriate legislation against the misuse of information and communication technologies for criminal or other purposes, including activities intended to affect the integrity of national critical infrastrucutres (CNI).)

5. SUBSCRIPTION TO IMPACT SERVICES:

We would be subscribed to the below services:

- ESCAPE
- NEWS
- GRC Mailing List
- IMPACT News Letter

6. ACCESS INFORMATION:

Public IP Address

Name

Telephone

Email

7. SIGNATORY:

I, the undersigned, have the power and authority to submit this application on behalf of my organization:

Name

Title

Date

Signature: