e-Crimes Questionnaire

Objective

This questionnaire has been prepared in connection with the HIPCAR project for "*Enhancing Competitiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures"* and the St. Vincent and the Grenadines national legislation on Electronic Crimes.

During the first phase of the HIPCAR project which involved extensive consultations with stakeholders of the Caribbean region, model legislative texts and policy guidelines were prepared.

These focused on the following areas:

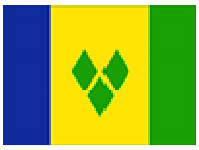
1. Information Society Issues including: *e-Commerce (Transactions); e-Commerce (Evidence); Cybercrimes/e-Crimes; Interception of Communications; Privacy and Data Protection and Access to Public Information (Freedom of Information)*

2. Telecommunications related to *Universal Access/Service; Interconnection and Access and Licensing*

Now in its second phase, HIPCAR has offered in-country assistance to beneficiary countries to transpose these model texts into national policies and legislations. In this regard, the Government of St. Vincent and the Grenadines has requested support from the project in the following work areas: *e-Commerce (Evidence) and Cybercrimes/e-Crimes.*

The relevant background information will be available for the stakeholders including the national legislations and HIPCAR model texts. These documents will be reviewed, discussed and adopted by consensus by participants at the upcoming Stakeholder Consultation to be held in St. Vincent from 18-20 June 2013.

This Questionnaire is designed to raise questions that will enable stakeholders and the team of consultants to obtain a complete understanding of the issues and interests to be considered in the process of legislative approval of the amendments to *Electronic Crimes.*




Questionnaire

Name: .....

Position/Title : .....

1. Which description best describes your organisation?

a. Financial/ Banking	b. Government	c. Information Technology
d. Telecommunication	e. Legal	f. Manufacturing
g. Retail	h. Transportation/Logistics	i. Other .....

2. Do you use computers, smartphones and/or data networks (internet and or intranet) as part of your business operations?
   ( ) Yes ( ) No

3. In what ways are computer systems and data networks utilised by your organisation.

   .....
   .....
   .....
   .....

4. Has your organisation experienced illegal access to the computer systems within the last year?
   ( ) Yes ( ) No ( ) I don't Know

5. The Electronic Crimes Act shall establish jurisdiction in which of the following areas?

   a. In the territory of St. Vincent and the Grenadines
   b. On a ship or aircraft registered in St. Vincent and the Grenadines
   c. By a national of St. Vincent and the Grenadines outside the jurisdiction of any country
   d. By a national of St. Vincent and the Grenadines outside the territory of St. Vincent and the Grenadines, if the person's conduct constitute an offence under a law of the country where the offence was committed
   e. All of the above

6. Do you think the unauthorised access to a computer system in whole or in part should be an offence under the Electronic Crimes Act? Please provide a reason for you answer.

( ) Yes ( ) No

.....
.....
.....

7. Do you think it should be an offence for an unauthorised person who accesses a computer system to remain logged into that computer system? Please provide a reason for you answer.

( ) Yes ( ) No

.....
.....
.....

8. Do you think it should be an offence for a person to intercept communications not meant for that person, to, from or within a computer system? Please provide a reason for you answer.

( ) Yes ( ) No

.....
.....
.....

9. Do you think that Child Pornography should also include audio files?

( ) Yes ( ) No

10. Do you think that the internet service provider should be legally obligated to monitor the information which they transmit or store for their users?

( ) Yes ( ) No

11. If a service provider (*internet service provider, access, hosting, caching or search engine provider*) receives concrete knowledge about illegal activities or content perpetrated by users of their services; what procedures must be followed:

    a. Remove the illegal content after having information of its existence within 24 hours

b. Inform the law enforcement officers of its existence to allow for further investigations
c. Send request to the subscriber who allegedly posted the content to remove it
d. No action should be taken without an order from the court
e. Other (please specify):

.....
.....
.....
.....

12. Identify the activities that should be offences under the Electronic Crimes Act.
    a. Illegal Remaining
    b. Data Espionage
    c. Computer related Fraud
    d. Computer related Forgery
    e. Identity-related crimes
    f. SPAM
    g. All of the above

13. Should there be a provision authorizing the use of sophisticated investigation tools such as remote forensic software under the Electronic Crimes Act?
    ( ) Yes ( ) No

    If yes, under what condition(s) would the use of such tools be appropriate?
    .....
    .....
    .....
    .....
    .....

Please specify any additional comments or questions you may have below

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

Thank you for your time and cooperation.