e-Crimes, Interception of Communications and e-Evidence

Policy Review and Regulations

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.Kitts-Nevis regulatory frameworks on *the Interception of Communication Act 2011, Electronic Crimes Act 2009 and the Evidence Bill 2010* and related documents.

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 to provide assistance to beneficiary countries to transpose these model texts into national policies and legislation. In this regard, the Government of St.Kitts & Nevis has requested support from the project in the following work areas: *e-Commerce (Evidence); Cybercrimes/e-Crimes and Interception of Communications.*

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.Kitts from 30-31 May 2011.

It is designed to raise questions that will enable stakeholders to engage in the regulatory framework process in an attempt to increase transparency, openness and fairness in government policies and regulations. In so doing, your responses will assist the team of consultants in obtaining a complete understanding of the issues and interests of various stakeholders to be considered that would inform the drafting process of the regulatory framework to accompany the *Electronic Crimes Act, Interception of Communications Act* and amendments to the *Electronic Evidence* Bill.

Questionnaire

Name of Person: .....
Position/Title : .....

1. Identify the industry that 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. Are you a user of computers, smartphones and 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. Which mechanism do you use to evidence that you were indeed the sender of your electronic communications?
   a. Write your name at the end of the message
   b. Use an electronic signature[1]
   c. Use biometrical[2] means
   d. None of the above
   e. Other (please specify) .....

---

[1]**Electronic signature** is an electronic means of codifying a data message so that it identifies the sender and makes it very difficult for persons other than the addressee to be able to read or change the data message; it is thus considered as a reliable means of providing safety, secrecy, and integrity to electronic communications.

[2]**Biometrical** means are biological (and electronic) means of identification of a person; for instance, fingerprints, iris, retina, are unique to each person, so the use of them as parameters to identify persons has been considered a safe way to instruct computer programs aimed at such identification.

5. In your opinion, which of the following practices should be used to verify the signature of the sender of an electronic communication?
    a. write your name at the end of the message
    b. use any form of electronic signature
    c. use certified electronic signature

    For the purpose of confidential information or highly sensitive transactions, which method would you accept, ranking the most acceptable first and least acceptable last?
    a. (i), (ii) and (iii)
    b. (ii), (iii) and (i)
    c. (iii), (ii) and (i)

6. What are do you consider to be the critical elements required to ensure that any electronic record or document and information are in fact authentic and the integrity has been preserved.

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

7. Who should be authorised to assign certified electronic signatures for the identification of individuals:
    a. Electronic Notaries only
    b. Duly registered public notaries
    c. Banks
    d. Public Bodies
    e. Certification Service Providers

8. In view of the critical role of the electronic authentication service providers, what should be the essential requirements that must be met by service providers in order to provide such services?

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

---

[3] **Certified (or "authenticated") electronic signature** is an electronic signature assigned to a person in accordance with strict procedures that ensure greater certainty on the identity of that person (who usually must appear before an e-notary or before a registered electronic authentication service provider to evidence his identity before being granted the electronic signature).

9. Do you think that all types of documents should be legally admissible in electronic form?
   ( ) Yes ( ) No

If no, please specify which electronic documents should not be legally admissible.
.....
.....
.....
.....

10. What should be the criteria for recognition of qualified electronic signature as authentic originating from outside the jurisdiction of St.Christopher & Nevis?
    a. Agreement must exist between the countries concerned
    b. Multilateral or bilateral international treaties
    c. Accredited international organisation attesting equivalence of criteria between countries
    d. Other (please specify):.....

11. Due to the rapid pace of technological advances in electronic signatures, what mechanisms can be used to ensure that electronic signatures issued today will remain valid in the future?
    a. digital time-stamping[4] should be legally required for all electronic signatures
    b. standardise technologies used for electronic signatures
    c. Other (please specify):

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

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

13. Do you think the mere unauthorised access to a computer system should be an offence under the Electronic Crimes Act? Give reason for your answer.
    ( ) Yes ( ) No

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

A [4]**digital time stamp** gives you proof that the contents of your work existed at a point-in-time and that the contents have not changed since that time. The procedures maintain complete privacy of your documents themselves. The result is *simple*, *secure*, *independent* and *portable* proof of electronic record integrity.

14. Which of these types of computer security incidents have been detected at your organisation within the last year? Circle the letter(s) to the corresponding answer.
    a. Computer Theft
    b. Sabotage of data or network
    c. SPAM
    d. Denial of Service (DoS)
    e. Computer related Fraud
    f. Data Espionage
    g. Virus (including worms and Trojans)
    h. Other (please specify).....

15. Identify some of the security technologies used by your organisation to protect against security incidents on your computer systems.
    a. Antivirus Software
    b. Firewalls (Software or hardware)
    c. Biometrics
    d. Smartcards
    e. Website Content Filtering
    f. Encryption / Cryptography for File Transfer
    g. Intrusion Prevention/ Detection System
    h. Virtual Private Networks (VPNs)
    i. Password Complexity
    j. Access Logs
    k. Other (please specify).....

16. Which security technologies do you consider to be most effective and would recommend to other organisations?

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

17. Identify some of the possible implications of the Interception of Communications Act on the use of encryption and anonymous communication technology.

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

18. Are there adequate backup and archiving procedures implemented in your organisation?
( ) Yes ( ) No

If yes, how often are they reviewed for accuracy and completeness?
.....

19. To facilitate the collection of electronic evidence that is admissible in a court of law, what measures should be taken by organisation to ensure that useful evidence is captured and preserve as part of incident management?

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

20. Given that traffic data can be modified or deleted even before an authorisation to order the preservation of data is issued to the service provider, do you think it is necessary to prescribe data retention obligations on service providers?
( ) Yes ( ) No

21. For expedited preservation of computer data in a criminal investigation, the notice issued by the authorised officer to the person in control of the computer system to preserve the data should be for a period of up to:
a. 5 days b. 7 days c. 10 days d. 14 days

22. 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):

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

23. Do you think that the service provider should be held liable, if illegal content is not removed after having information confirming its existence?
    ( ) Yes ( ) No

24. Should there be a code of conduct or standards appointed for internet service providers and telecommunications service providers with regards to data transmitted electronically through their computer networks?
    ( ) Yes ( ) No

    If yes, what are some essential elements that should be included in the code of conduct?

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

25. Identify the activities that should be offences under the Electronic Crimes Act 2009.
    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

26. Should there be a provision authorizing the use of sophisticated investigation tools such as remote forensic software under the Electronic Crimes Act 2009?
    ( ) Yes ( ) No

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

27. Do you see any reason for a change in the way you conduct business using communication networks as a result of the Interception of Communications Act?

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

28. With regards to the implementation of the Interception Act, how can government best support you to minimise the impact on your business?

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

29. Under the Interception of Communications Act, what safeguard measures should be taken into consideration in order to protect the rights of individual from unlawful interception?

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

30. An interception warrant shall be valid for an initial period, not exceeding:
    a. 14 days
    b. 30 days
    c. 90 days
    d. More than 90 days

31. Which types of professional secrecy shall remain privilege and not disclosed without consent of the persons if evidence is obtained by interception;
    a. medical secrecy
    b. bank secrecy
    c. communications of professional character between attorney-at-law and client
    d. financial secrecy
    e. trade secret
    f. none of the above
    g. Comments (if any) .....

    .....
    .....

32. Do you think the Interception of Communication Act should be amended to provide for the allocation of costs incurred by the communications provider?
    ( ) Yes ( ) No

If yes, which of the following mechanisms would you consider for the allocation of costs?

a. establish a mechanism for costs to be shared between Government of St.Kitts & Nevis and the communications provider;
b. the communications provider will pay the cost incurred that enable interception and or store communications including investment, technical, maintenance and operating costs and for Government to reimburse for the direct costs of personnel and administration
c. Government will pay for all costs incurred in interception
d. Other (please specify):

.....
.....

33. Should there be indemnity provisions for communication service providers acting in response to an interception warrant?
( ) Yes ( ) No

34. In light of the Interception of Communications Code of Conduct or Practice, what are some of the critical elements you would like to see included in the document?

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

35. Should an independent authority be created with the power to provide guidance and control to ensure that the interception of communication is conducted in accordance with legal authorization?
( ) Yes ( ) No

If no, which of the following entities would be most suitable to monitor communication interception?

a. National Telecommunications Regulatory Commission (NTRC)
b. Department of Information Technology
c. The Ombudsman
d. Ministry of Justice & Legal
e. Other (please specify)…….

36. Select the areas in which the Electronic Crimes Act 2009 shall establish jurisdiction:
    a. In the territory of St.Christopher & Nevis
    b. On a ship or aircraft registered in St.Christopher & Nevis
    c. By a national of St.Christopher & Nevis outside the jurisdiction of any country
    d. By a national of St.Christopher & Nevis outside the territory of St.Christopher & Nevis, if the person's conduct constitute an offence under a law of the country where the offence was committed
    e. All of the above

37. Which of the following entities should be responsible for the monitoring and investigating cybercrimes and related matters?
    a. Create an ICT Crimes Unit or Computer Incident Response Team (CIRT) within the St.Christopher & Nevis Police Force
    b. Department of Information Technology
    c. Establish a regional e-Crimes investigation body
    d. Collaborate with international e-Crimes Unit or CIRT
    e. All of the above
    f. Other.....

38. What mechanisms can be established to encourage formal cooperation with other countries in the fight against cybercrime?

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

Please specify any additional comments or questions you may have below

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

Thank you for your time and cooperation.