MEETINGS OF MINISTERS OF JUSTICE OR
OF MINISTERS OR ATTORNEYS GENERAL
OF THE AMERICAS

OEA/Ser.K/XXXIV
CIBER-VI/doc.3/09
17 November 2009
Original: English

Sixth Meeting of the Working Group on Cyber-Crime
January 21 and 22, 2010
Washington, D.C.

PREPARATORY QUESTIONNAIRE OF THE SIXTH MEETING OF THE WORKING GROUP ON CYBER-CRIME

INTRODUCTION

The object of this questionnaire is to collect useful information for the purposes of the Sixth Meeting of the Working Group on Cyber-Crime, with regard to the recommendations that have been put forward at previous meetings and been adopted in the framework of the process of Meetings of Ministers of Justice or other Ministers or Attorneys General of the Americas (REMJA), which are in accordance therewith.

To that end, the questionnaire is divided into four thematic areas: (1) Legislation; (2) Specialized Units and Bodies; (3) International Cooperation; and (4) Training.

Bearing the foregoing in mind, kindly submit the response of your State to this questionnaire by e-mail (LegalCooperation@oas.org) or fax (+ (202) 458-3598) to the OAS General Secretariat (Department of Legal Cooperation, Secretariat for Legal Affairs) by **December 10, 2009**.

Please use any extra space that might be required for each response, or attach additional pages, as necessary.

I. LEGISLATION

1.1. Has your country adopted laws to prevent, investigate, and punish cyber-crime? Yes (X) No ( )

If so, please list and enclose a copy, preferably electronic, of those laws: **The Criminal Code - 2004**

Has your country criminalized the following types of cyber-crime?

a) Illegal access	Yes (X) No ( )
b) Illegal interception	Yes ( ) No ( )
c) Data interference	Yes (X) No ( )
d) System interference	Yes ( ) No ( )
e) Misuse of devices	Yes (X) No ( )
f) Computer-related forgery	Yes (X) No ( )
g) Computer-related fraud	Yes (X) No ( )
h) Child pornography	Yes (X) No ( )
i) Offences related to infringements of copyright and related rights	Yes (X) No ( )
j) Other offences (please list): _____	Yes ( ) No ( )

If so, kindly provide a brief description of the provisions and/or other measures in place together with a copy, preferably electronic, thereof:

Primarily computer misuse and data recovery.

If your country has criminalized any of the above conduct, briefly mention the results that have been obtained in that regard, such as judicial proceedings undertaken and their outcome:

Not Applicable

If your country has not criminalized any of the above conduct, please mention what steps, if any, it has taken to do so:

- **Workshops.**
- **Specific legislation to be implemented.**
- **Investigators and Prosecutors to be trained.**

Has your country adopted substantive or procedural legislation or other necessary measures to enable it to obtain and preserve evidence in electronic form of any criminal offence? Yes ( ) **No (X)**

If so, kindly provide a brief description of the provisions and/or other measures in place in that regard, together with a copy, preferably electronic, thereof:

Not Applicable

1.2. Has your country adopted substantive or procedural legislation or other necessary measures to enable the admissibility in criminal investigations and proceedings of evidence in electronic form? **Yes (X)** No ( )

If so, kindly provide a brief description of the provisions and/or other measures in place in that regard, together with a copy, preferably electronic, thereof:

Telecommunications evidence admissible. Can be proved by affidavit.

1.3. Has your country adopted substantive or procedural legislation or other necessary measures whereby its competent authorities can:

a) Order a person in its territory to provide information in their possession or control, which is stored in a computer system or a computer-data medium? **Yes (X)** No ( )

b) Order a service provider (e.g. an ISP) offering its services in its territory to release subscriber information in its possession or control relating to such services? Yes ( ) **No (X)**

If so, kindly provide a brief description of the provisions and/or other measures in place in that regard, together with a copy, preferably electronic, thereof: **Same as 1.2 above.**

1.4. Has your country adopted substantive or procedural legislation or other necessary measures whereby its competent authorities can:

a) Seize, confiscate, or attach computer systems or computer-data storage media? Yes (X) No ( )
b) Copy and keep the computer data accessed? Yes ( ) No (X)
c) Maintain the integrity of the stored computer data? Yes ( ) No (X)
d) Render inaccessible or remove the data in the accessed system? Yes ( ) No (X)

If so, kindly provide a brief description of the provisions and/or other measures in place together with a copy, preferably electronic, thereof:

Not Applicable.

Has your country adopted substantive or procedural legislation or other necessary measures whereby its competent authorities can obtain and intercept traffic and content data of specified communications transmitted in its territory via computer systems? Yes ( ) No (X)

If so, kindly provide a brief description of the provisions and/or other measures in place in that regard, together with a copy, preferably electronic, thereof: **Not Applicable**

II. SPECIALIZED UNITS

2.1. Has your country established specialized units or agencies specifically charged with the investigation and prosecution of computer crimes? Yes ( ) No (X)

If so, please supply the following information: **Not Applicable**

- Name of the unit or agency: _____
- Institution to which it reports: _____
- Contact information:
  - Name of contact: _____
  - Address: _____
  - Telephone(s): _____ Fax: _____
  - E-mail address: _____

2.2. Has your country established specialized units or agencies specifically charged with the prosecution of computer crimes? Yes ( ) No (X)

If so, please supply the following information: **Not Applicable.**

- Name of the unit or agency: _____
- Institution to which it reports: _____
- Contact information:
  - Name of contact: _____
  - Address: _____
  - Telephone(s): _____ Fax: _____
  - E-mail address: _____

2.3. What measures has your country adopted to strengthen relations between the authorities responsible for the investigation and prosecution of cyber-crime and the private sector, especially companies that provide information and communication technology services, in particular Internet services? _____

III. INTERNATIONAL COOPERATION

3.1. Has your country acceded to the Council of Europe Convention on Cybercrime? Yes ( ) No (X)

If not, has your country considered application of the principles contained in that Convention? Yes ( ) No ( ) Unsure (X)

If so, please describe what that consideration has entailed: _____

3.2. Has your country joined the G8 24/7 High Tech Crime Network? Yes ( ) No (X)

If not, has your country taken any steps to join it? Yes ( ) No (X)

If so, please describe those steps: _____

Has your country adopted laws or other measures that enable processing of requests for mutual assistance from other states which, in conformity with their domestic laws, have the power to investigate or prosecute computer crimes? Yes (X) No ( )

If so, kindly provide a brief description of the provisions and/or other measures in place in that regard, together with a copy, preferably electronic, thereof:

Treaty with Commonwealth and American jurisdictions on Mutual Assistance in Criminal Matters.

3.3. Has your country adopted laws or other measures that enable processing of requests for mutual assistance from other states for the purpose of obtaining evidence in electronic form and taking other steps necessary to facilitate the investigation or prosecution of computer crimes? Yes ( ) No (X)

If so, kindly provide a brief description of the provisions and/or other measures in place in that regard, together with a copy, preferably electronic, thereof: _____

3.4. Has your government presented or received requests for mutual assistance for the investigation or prosecution of computer crimes or for the purpose of obtaining evidence in electronic form and taking other steps necessary to facilitate the investigation or prosecution of computer crimes? **Yes (X)** No ( )

If so, please indicate the number of requests presented and/or received and the status of those requests:

Unable to provide precise information at this time.

IV. TRAINING

4.1. Does your country provide training to law enforcement personnel on computer crimes and the collection of electronic evidence? Yes ( ) **No (X)**

If so, please provide a brief description on the type of training and number of personnel trained: _____

4.2. Does your country provide training prosecutors on computer crimes and the collection of electronic evidence? Yes ( ) **No (X)**

If so, please provide a brief description on the type of training and number of personnel trained: _____

4.3. Regarding your country's efforts to provide training on investigating and prosecuting crimes involving computers and the Internet, please describe your country's goals for the next two years and the necessary conditions to achieve those goals:

Not Applicable.

4.4. Has your country sent officials to workshops presented by the Working Group on Cyber-crime? **Yes (X)** No ( )

If so, please provide a brief description of who has participated in these workshops, whether the workshops have provided useful training, and how the participants have applied this training in their work:

Crown Counsel, Police Prosecutors, Police Investigators.

4.5. Please provide recommendations on the most important topics related to computer crime and electronic evidence that should be incorporated into Working Group workshops for the next two years:

Obtaining and preserving prosecution of Cyber Crime.

4.6. Within the mandates of the REMJA, please provide recommendations on how the Working Group on Cyber-crime can best assist your country in developing or enhancing its ability to address crimes involving computers and the Internet:

Training and Government awareness.

INFORMATION ON THE OFFICIAL RESPONSIBLE FOR COMPLETION OF THIS QUESTIONNAIRE

Please provide the following information:

(a) State: **SAINT LUCIA**
(b) The official to be consulted regarding the responses to the questionnaire is:
(c) **Mr. SERYOZA. CENAC**
Title/position: **Crown Counsel**
Agency/office: **Crown Prosecution Service/ Office of Director of Public Prosecutions**
Address: **Micoud Street, Castries, Saint Lucia.**
Telephone number: 1 758 468 6116 / 1 758 452 3636
Fax number: 1 758 459 0235
E-mail address: slucps@gmail.com