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

Eighth Meeting of the Working Group on Cyber-crime

OEA/Ser.K/XXXIV
CIBER-VIII/doc.1/11
6 November 2013
Original: English

PREPARATORY QUESTIONNAIRE FOR THE EIGHTH MEETING OF THE WORKING GROUP ON CYBER-CRIME

INTRODUCTION

The object of this questionnaire is to collect useful information for the purposes of the Eighth Meeting of the Working Group on Cyber-Crime, which will take place in early 2014, with regard to the recommendations that have been put forward at previous meetings and that 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 five thematic areas: (I) Legislation; (II) International Cooperation; (III) Specialized Units and National Efforts; (IV) Results of Cyber-Crime Investigations and Prosecutions; and (V) 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 **Tuesday, December 10, 2013.**

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

I. LEGISLATION

A. SUBSTANTIVE LEGISLATION:

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

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

If you answered yes to any of the foregoing, please list and enclose a copy, preferably electronic, of those laws: _____

_____

_____

1.2. Has your country implemented legislation which:

a) Criminalizes the attempted commission of any of the above-noted types of cyber-crime? Yes (✓) No ( )

If so, please list and enclose a copy, preferably electronic, of those laws: _____

b) Criminalizes aiding and abetting in the commission of any of the above-noted types of cyber-crime? Yes (✓) No ( )

If so, please list and enclose a copy, preferably electronic, of those laws: _____

c) Contemplates the possibility of corporate responsibility for cyber-crimes, i.e., legislation wherein legal persons can be held responsible for criminal offenses related to cyber-crime? Yes ( ) No (✓)

If so, please list and enclose a copy, preferably electronic, of those laws: _____

B. PROCEDURAL LEGISLATION:

1.3. If your country does not have a cyber-crime law that criminalizes any of the above conduct, are there currently any efforts to enact such laws: Yes ( ) No ( )

If so, please describe those efforts: Uncertain about any efforts ongoing

1.4. Does the legislation of your country allow criminal investigators to compel Internet Service Providers to preserve electronic evidence without the need for a court order?

Yes ( ) 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: _____

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

a) Seize, confiscate, or attach computer systems or computer-data storage media? Yes (✓) No ( )

b) Copy and keep the computer data accessed? 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: s. 18 & 19 Electronic Crimes Act 2013

II. INTERNATIONAL COOPERATION

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

If not, has your country taken any steps to join it? Yes ( ) No ( ) Do Not Know (✓)

If so, please describe those steps: _____

2.2. Do the laws of your country allow for the processing of requests for mutual assistance from other states for the purpose of obtaining evidence in electronic form?

Yes (✓) No ( ) Do Not Know ( )

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: _____

2.3. Has your government presented or received requests for mutual assistance for the investigation or prosecution of cyber-crimes or for the purpose of obtaining evidence in electronic form and taking other steps necessary to facilitate the investigation or prosecution of cyber-crimes? Yes ( ) No ( ) Do Not Know (✓)

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

III. SPECIALIZED UNITS & NATIONAL EFFORTS

3.1. Is there a specialized unit or agency in your country specifically charged with the **investigation** of cyber-crimes? (police authority) Yes (✓) No ( )

If so, please supply the following information:

- Name of the unit or agency: Regional Cyber Investigation Laboratory
- Institution to which it reports: Commissioner of Police (Deputy)
- Internet address of the unit or agency: _____
- Contact information:
  - Name of contact: Mrs. Gordina Hector - Murrell
  - Address: Langford, St. John's, Antigua
  - Telephone(s): 562 - 7647 Fax: 562 - 7657
  - E-mail address: rcil_antigua@antigua.gov.ag

3.2. Is there a specialized unit or agency in your country specifically assigned the responsibility of **prosecuting** cyber-crimes? Yes ( ) No (✓)

If so, please supply the following information:

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

3.3. Has your country established any Internet pages to provide citizens with information on how to avoid falling prey to cybercrimes and on how to detect and report such crimes to competent authorities when they do occur?

Yes ( ) No (✓)

If so, kindly provide the respective Internet address/es of the page/s, as well as a brief description of the website/s: _____

_____

_____

3.4. Has your country implemented any probity or awareness-raising programs on the dangers of cyber-crime, or produced manuals or guides to orient and alert the public on the dangers of cyber-crime and how to avoid becoming a victim thereof:

Yes ( ) No (✓)

If so, kindly provide a brief description of those programs, manuals, or guides: _____

_____

_____

IV. RESULTS OF CYBERCRIME INVESTIGATIONS AND PROSECUTIONS

4.1. Please indicate the number of **investigations** that your country has carried out with respect to each of the following cyber-crime offenses or conduct, from January, 2012 to the present:

a) Illegal access — Number of investigations: 0
b) Illegal interception — Number of investigations: 0
c) Data interference — Number of investigations: 0
d) System interference — Number of investigations: 0
e) Misuse of devices — Number of investigations: 0
f) Computer-related forgery — Number of investigations: 0
g) Computer-related fraud — Number of investigations: 0
h) Child pornography — Number of investigations: 1
i) Offences related to infringements of copyright and related rights — Number of investigations: 2

4.2. If your country has criminalized any of the cyber-crime offenses referred to in question 1.1, above, please indicate the number of **prosecutions** that your country has carried out with respect to each of the corresponding cyber-crime offenses, from January, 2012 to the present, as well as the number of cases that resulted in a **conviction**:

a) Illegal access — Cases prosecuted: 0 Convictions 0
b) Illegal interception — Cases prosecuted: 0 Convictions 0
c) Data interference — Cases prosecuted: 0 Convictions 0
d) System interference — Cases prosecuted: 0 Convictions 0
e) Misuse of devices — Cases prosecuted: 0 Convictions 0
f) Computer-related forgery — Cases prosecuted: 0 Convictions 0
g) Computer-related fraud — Cases prosecuted: 0 Convictions 0
h) Child pornography — Cases prosecuted: 0 Convictions 0
i) Offences related to infringements of copyright and related rights — Cases prosecuted: ____ Convictions ____ pending

4.3. Have you encountered any difficulties with respect to the investigation and/or prosecution of the above offenses? Yes (✓) No ( )

If so, please provide a detailed and specific description of the type of difficulties that have been encountered: 1. The time it takes to complete investigations
2. The need for modern computer forensic equipment to meet the changing technology.

4.4. Are there any areas related to the fight against cyber-crime in which your country could benefit from technical cooperation provided by other Member States? Yes (✓) No ( )

If so, please provide a detailed and specific description of the type of technical cooperation that would be of benefit to your country:
- computer forensic training and equipment
- investigation techniques related thereto

V. TRAINING

5.1. Does your country provide training to law enforcement personnel on cyber-crimes and the collection of electronic evidence? Yes (✓) No ( )

If so, please provide a brief description on the type of training and number of personnel trained: Examination of the legislation and its implementation. Not sure of the number of persons

5.2. Does your country provide training to prosecutors on cyber-crimes and the collection of electronic evidence? Yes (✓) No ( )

If so, please provide a brief description on the type of training and number of personnel trained: Examination of the provisions of the legislation and implementation of the same

5.3. Does your country provide training to judges on cyber-crimes and the collection of electronic evidence? Yes (✓) No ( )

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

INFORMATION ON THE OFFICIAL RESPONSIBLE FOR COMPLETION OF THIS QUESTIONNAIRE

Please provide the following information:

(a) State: ANTIGUA AND BARBUDA
(b) The official to be consulted regarding the responses to the questionnaire is:
( ) Mr.:
(✓) Ms.: SHANNON SONES
Title/position: CROWN COUNSEL II
Agency/office: OFFICE OF THE DIRECTOR OF PUBLIC PROSECUTIONS
Address: PARLIAMENT DRIVE, ST. JOHN'S, ANTIGUA
Telephone number: 268-462-2464
Fax number: 268-460-8700
E-mail address: dppantigua@gmail.com