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

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

Eighth Meeting of the Working Group on Cyber-crime

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 (x)
g) Computer-related fraud — Yes ( ) No (x)
h) Child pornography — Yes (√) No ( )
i) Offences related to infringements of copyright and related rights — Yes ( ) No (x)
j) Other offences (please list): **Disclosure of access codes [section 8 (1) Computer Misuse Act, 2000]** — Yes (√) No ( )

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

Computer Misuse Act, 2000; Interception of Communications Act Chap. 15:08; Children Act 2012; Data Protection Act 2011 *(attached).*

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:
Computer Misuse Act, 2000; Interception of Communications Act Chap. 15:08; Children Act 2012; Data Protection Act 2011 *(attached).*

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:
Accessories and Abettors Act Chap. 10:02 *attached).*

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:
A Cybercrime Bill has been drafted and includes corporate liability
This Bill identifies *inter alia,* an offence by a body corporate.

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:

The draft Cybercrime Bill 2013 is currently under review by the Government and it is anticipated that the legislation will be enacted in 2014.

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 (**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: **Provisions to facilitate this process are included within the proposed Cybercrime Bill 2013 under the section "Internet Service Providers."**

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 (**x**)

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

(a) Computer Misuse Act 2000 (*e.g.* Sections 15-16 "Saving for investigation by police officer" & "Power of Police Officer to access computer program and access data"),

(b) Proposed Cybercrime Bill 2013 (*e.g.* Part III "Enforcement")

II. INTERNATIONAL COOPERATION

2.1. 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 ( ) 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: **Mutual Assistance in Criminal Matters Amendment Act, 2004 (*e.g.* "Mutual Provision of Evidence" - Sections 33E "Form of testimony" and 33F "Admission of Foreign Evidence.")**

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:

Relevant information to be provided in due course.

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: **Trinidad and Tobago Police Service Cybercrime Unit.**
- Institution to which it reports: **Trinidad and Tobago Police Service**
- Internet address of the unit or agency: **http://www.ttps.gov.tt/**
- Contact information:
  - Name of contact: **Amos Sylvester**
  - Address: **Police Administration Building, Sackville Street, Port of Spain**
  - Telephone(s): **(868) 623-8429** Fax: _____
  - E-mail address: **_sylvester@ttps.gov.tt**

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

The Trinidad and Tobago Police Service and the Office of the Director of Public Prosecutions have the responsibility of prosecuting all crimes.

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 (**x**)

There are plans by the Government to implement such initiatives within the first quarter of 2014.

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:

There are public awareness initiatives which are conducted by the Telecommunications Authority of Trinidad and Tobago, the Trinidad and Tobago Police Service, the Internet Society Trinidad and Tobago Chapter, and other private sector companies, including the banking sector.

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

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

Statistical information for 4.1 and 4.2 will be provided in due course.

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:

There is a need for greater capacity to investigate and prosecute such crimes, as well as a need for the Cybercrime Bill to be enacted in order to criminalize these offences.

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:

Capacity building for law enforcement, prosecutors and the judiciary; awareness raising, including public awareness, and developing child online protection strategies; training and certification of nationals in information security,

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:

Please refer to paragraph 5.3 *infra.*

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:

Please refer to paragraph 5.3 *infra.*

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:

Officers of the Trinidad and Tobago Police Service and the Office of the Director of Public Prosecutions have been exposed to training conducted by international organizations. In developing the cybercrime legislation, the Government has held sensitization sessions with members of the Judiciary and the DPP's Office in order to gain feedback and input on said legislation. The Government has also identified capacity building for law enforcement, prosecutors and judges as a priority and as such is working towards the conduct of training and awareness sessions in the first quarter of 2014.

INFORMATION ON THE OFFICIAL RESPONSIBLE FOR COMPLETION OF THIS QUESTIONNAIRE

Please provide the following information:

(a) State: **Trinidad and Tobago**
(b) The official to be consulted regarding the responses to the questionnaire is:
( ) Mr.:_
( ) Ms.: **Joan R. Furlonge**
Title/position: **Legal Advisor to the Attorney General**
Agency/office: **Ministry of the Attorney General.**
Address: **Cabildo Chambers, 6th Floor, 23-27 St. Vincent Street, Port of Spain.**
Telephone number: **(868) 625-5505 Extension 2646.**
Fax number: **(868) 625-6578**
E-mail address: **jrfurlonge@ag.gov.tt; jrfurlonge@gmail.com**