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 (**x**)
b)	Illegal interception	Yes ( ) No (**x**)
c)	Data interference	Yes ( ) No (**x**)
d)	System interference	Yes ( ) No (**x**)
e)	Misuse of devices	Yes ( ) No (**x**)
f)	Computer-related forgery	Yes ( ) No (**x**)
g)	Computer-related fraud	Yes ( ) No (**x**)
h)	Child pornography	Yes ( ) No (**x**)
i)	Offences related to infringements of copyright and related rights	Yes ( ) No (**x**)
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: **The Electronic Crimes Act 23/2013 will have this effect when a date has been set for the Act to take effect.**

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 (**x**)

If so, please list and enclose a copy, preferably electronic, of those laws: **_The Electronic Crimes Act 23/2013 will have this effect when implemented.**

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

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 (**x**)

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: The Electronic Crimes Act 23/2013 has been passed and gazette. However, the date for the Act to take effect has not been set. When that is completed the offences as stated above will be criminalized.

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: _____
_____
_____

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 (**x**) No ( )

b) Copy and keep the computer data accessed? Yes (**x**) No ( )

If so, kindly provide a brief description of the provisions and/or other measures in place together with a copy, preferably electronic, thereof: The measures as stated at 1.5(a) and (b) are usually utilized by the Royal Grenada Police Force for investigation purposes.

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 (**x**) 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 (**x**) 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: **The Electornic Crimes Act 23/2013 will make this a reality.**

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 (**x**) 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 **(x)** No ( )

If so, please supply the following information:

- Name of the unit or agency: Royal Grenada Police Force
- Institution to which it reports: _____

- Internet address of the unit or agency: _____
- Contact information:
    - Name of contact: Winston James; Commissioner of Police
    - Address: St Georges Grenada_
    - Telephone(s): 440-3999 Fax: _____
    - E-mail address: _____

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

If so, please supply the following information:

- Name of the unit or agency: Office of the Director of Public Prosecutions
- Institution to which it reports: _____
- Internet address of the unit or agency: cnelson@spiceisle.com
- Contact information:
    - Name of contact: Christopher Nelson.
    - Address: Upper Church Street.
    - Telephone(s): 435-5566/5372_ Fax: 435-5624.
    - E-mail address: christophernelson81@gmail.com.

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**)

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 (**x**) No ( )

If so, kindly provide a brief description of those programs, manuals, or guides: **_SEE ATTACHMENT.**

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: **_nil_**
b) Illegal interception — Number of investigations: **_nil**
c) Data interference — Number of investigations: **_nil_**

d) System interference — Number of investigations: **_nil_**
e) Misuse of devices — Number of investigations: **_nil_**
f) Computer-related forgery — Number of investigations: **_nil_**
g) Computer-related fraud — Number of investigations: **_nil_**
h) Child pornography — Number of investigations: **_nil_**
i) Offences related to infringements of copyright and related rights — Number of investigations: **_nil_**

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**: **N/A**

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 _____

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

If so, please provide a detailed and specific description of the type of difficulties that have been encountered: **N/A**

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 (**X**) No ( )

If so, please provide a detailed and specific description of the type of technical cooperation that would be of benefit to your country:

The requirement has always been for resources. Prosecutors and police investigators have attended workshops/seminars relating to the matter under discussion and the major complaint has been not the content of the workshops but inability to the implement what they have learnt due to insufficient or no resources.

V. TRAINING

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

If so, please provide a brief description on the type of training and number of personnel trained:
See page 7

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

If so, please provide a brief description on the type of training and number of personnel trained: **See pg 7**

5.3. Does your country provide training to judges on cyber-crimes and the collection of electronic evidence? Yes ( ) No ( ) **Not Aware of Any**.

If so, please provide a brief description on the type of training and number of personnel trained: **The judges in the jurisdiction have not attended any conferences**.

INFORMATION ON THE OFFICIAL RESPONSIBLE FOR COMPLETION OF THIS QUESTIONNAIRE

Please provide the following information:

(a) State:_THE TRI-ISLAND STATE OF GRENADA, CARRIACOU AND PETIT MARTINIQUE.
(b) The official to be consulted regarding the responses to the questionnaire is:
( ) Mr.:_____
( ) Ms.:Dionne Lawrence-Pivotte.
Title/position: Legal Counsel
Agency/office: Office of the Director of Public Prosecutions.
Address: Upper Church Street, St Georges, Grenada.
_____
Telephone number: 1-473-435-5566/5372; 1-473-415-1695
Fax number: 1 473-435-5624_
E-mail address: dionne_lwrnc@yahoo.com.

Question 3.4

In 2012 and 2013, the National Telecommunications Regulatory Commission (NTRC) in collaboration with other stakeholders embarked on a Cyber Security Initiative/Children Online Protection targeting parents in parishes throughout Grenada & Carriacou. This programme was an interactive session in each parish educating parents on the cyber dangers/online dangers, tips for protecting their children (commonly used slangs by children when communicating with friends), how to deal with cyber bullying and online predator and online crimes(identify theft, phishing).
The program included capacity building and awareness to parents, videos on cyber dangers, handouts and brochures which provided tips for protecting children from online predators.
In addition, parents were also educated on components of the newly enacted cyber crime bill.
The NTRC believes that continued awareness about cyber security is important and will continue to embark on initiative extending the programme to the primary and secondary schools throughout Grenada and Carriacou.

V. TRAINING

5.1 Type of training provided included **Seized Computer Evidence Recovery Specialist Training.** It involved extracting information from computer hard drives. It was sponsored by the United States Department of Treasury. Also, **Cybercrime Legislation Drafting Workshop** sponsored by The Organization of American States, United States Department of Justice, United States Department of State, and Council of Europe.

Number of Personnel attended: 1

5.2 Type of training provided included:
Cyber Awareness Seminars For Prosecutors. The topics of discussion included; Investigation, Terrorist use of Internet, Seizure and Analysis of Digital Evidence, Using Digital Evidence in Court, Human Rights and Community Enjoyment, Legal Processes to Obtaining Digital Evidence, Understanding Local Capacity. It was conducted by Anti Terrorism Assistance Program United States Bureau of Diplomatic Security; United States Department of State.
Hemispheric Workshop in Cyber Security and Cyber Crime: **Regional Coordination and Information Sharing** discussion on Forensics, Working with Internet Service Providers, Developing National Computer Emergency Readiness Team(CERT) and Terrorist use of Internet. It was conducted by Organisation of American States and Inter American Convention Against Terrorism.
Number of Personnel Attended: 1