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

OEA/Ser.K/XXXIV
CIBER-VII/doc.1/11
14 November 2011
Original: English

Seventh Meeting of the Working Group on Cyber-crime

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

INTRODUCTION

The object of this questionnaire is to collect useful information for the purposes of the Seventh Meeting of the Working Group on Cyber-Crime, which will take place at OAS Headquarters on February 6 and 7, 2012, 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 four thematic areas: (1) Legislation; (2) Specialized Units and National Efforts; (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 **Friday, December 16, 2011.**

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 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. 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: _____

_____

_____

1.3. Do the emergency laws or other emergency measures in your country permit 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: _____

_____

_____

1.4. 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 ( ) 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: _____

_____

_____

1.5. Do the procedural laws in your country allow for the lawful interception of electronic communications transmitted in its territory via computer systems? 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: _____

_____

_____

II. SPECIALIZED UNITS & NATIONAL EFFORTS

2.1. Is there a specialized unit or agency in your country specifically charged with the investigation of computer crimes? (police authority) 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: _____

2.2. 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: _____

2.3. 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: _____

_____

_____

2.4. Has your country developed and/or implemented a national cyber-security strategy that includes efforts to deter, investigate and prosecute cybercrime, as part of a broader and more coordinated effort to protect the computers and networks of their citizens?

Yes ( ) No (✓)

If so, kindly provide a brief description of that strategy: _____

_____

_____

III. INTERNATIONAL COOPERATION

3.1. Has your country acceded to the Council of Europe Convention on Cybercrime?

Yes ( ) No (✓)

If not, has your country considered applying any of the principles contained in that Convention?

Yes ( ) No (✓) Do Not Know ( )

If so, please describe what that consideration has entailed: There has been discussions by National Security Personnell on the need for legislation + training on cyber crimes

3.2. 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: _____

3.3. 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: _____

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 ( ) No ( ) Do Not Know ( )

If so, please indicate the number of requests presented and/or received and the status of those requests: 2 completed requests.

IV. TRAINING

4.1. Does your country provide training to law enforcement personnel on computer 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: _____

4.2. Does your country provide training to prosecutors on computer 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: _____

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: _____

4.4. Has your country sent officials to workshops presented by the Working Group on Cyber-crime? Yes (✓) No ( ) Do Not Know ( )

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: Two Crown Counsels from the office of Director of Public Prosecutions attended workshops. Useful training but the ~~staff~~ absence of legislation limits them ability to apply the training.

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: _____

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: Providing ~~draft~~ legislative support and training on the area of cyber crime.

INFORMATION ON THE OFFICIAL RESPONSIBLE FOR COMPLETION OF THIS QUESTIONNAIRE

Please provide the following information:

(a) State: GRENADA

(b) The official to be consulted regarding the responses to the questionnaire is:

(x) Mr.: ROHAN PHILLIP

( ) Ms.:

Title/position: ATTORNEY GENERAL

Agency/office: MINISTRY OF LEGAL AFFAIRS

Address: 414 HA BLAIZE STREET
ST. GEORGE'S GRENADA

Telephone number: 1-473-440-2050

Fax number: 1-473-435-2964

E-mail address: legalaffairs@spiceisle.com

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

Seventh Meeting of the Working Group on Cyber-crime

OEA/Ser.K/XXXIV
CIBER-VII/doc.1/11
14 November 2011
Original: English

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

INTRODUCTION

The object of this questionnaire is to collect useful information for the purposes of the Seventh Meeting of the Working Group on Cyber-Crime, which will take place at OAS Headquarters on February 6 and 7, 2012, 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 four thematic areas: (1) Legislation; (2) Specialized Units and National Efforts; (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 **Friday, December 16, 2011.**

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 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. 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: Legislations have been drafted and awaiting approval. Proposed to pass during 2012.

1.3. Do the emergency laws or other emergency measures in your country permit 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: _____

1.4. 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 ( ) 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: New legislation will provide Mechanism to address above contents.

1.5. Do the procedural laws in your country allow for the lawful interception of electronic communications transmitted in its territory via computer systems? 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: _____

II. SPECIALIZED UNITS & NATIONAL EFFORTS

2.1. Is there a specialized unit or agency in your country specifically charged with the investigation of computer crimes? (police authority) Yes (✓) 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: www.rgpf.gd
- Contact information:
  - Name of contact: Commissioner of Police, Mr. Willan Thompson
  - Address: Police Headquarters, Fort George, St Georges
  - Telephone(s): 473 440-2823 Fax: 440-4139
  - E-mail address: rgpf@spiceisle.com

2.2. 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: Department of Public Prosecution
- Institution to which it reports: _____
- Internet address of the unit or agency: _____
- Contact information:
  - Name of contact: Mr. Christopher Nelson
  - Address: Upper Church St. St Georges
  - Telephone(s): 473-435-5566 Fax: 435-5624
  - E-mail address: legalaffairs@spiceisle.com

2.3. 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: _____

2.4. Has your country developed and/or implemented a national cyber-security strategy that includes efforts to deter, investigate and prosecute cybercrime, as part of a broader and more coordinated effort to protect the computers and networks of their citizens?

Yes ( ) No (✓)

If so, kindly provide a brief description of that strategy: _____

III. INTERNATIONAL COOPERATION

3.1. Has your country acceded to the Council of Europe Convention on Cybercrime?

Yes ( ) No (✓)

If not, has your country considered applying any of the principles contained in that Convention?

Yes ( ) No ( ) Do Not Know (✓)

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 (✓)

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

If so, please describe those steps: _____

_____

_____

3.3. 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: _____

_____

_____

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 ( ) No ( ) Do Not Know (✓)

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

_____

_____

IV. TRAINING

4.1. Does your country provide training to law enforcement personnel on computer 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: _____

4.2. Does your country provide training to prosecutors on computer 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: _____

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: No known goals

4.4. Has your country sent officials to workshops presented by the Working Group on Cyber-crime? Yes (✓) No ( ) Do Not Know ( )

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: Francisca Noel and Jason Hadley (Police Officials). Both has expressed positive feedback and insights into cyber crime. Recommendations have been made for action of higher authorities.

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: Research on trends and threats to developing nations, national and regional integration for Cyber security

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: Need for training for Police and Prosecutors, computer equipment to facilitate training

INFORMATION ON THE OFFICIAL RESPONSIBLE FOR COMPLETION OF THIS QUESTIONNAIRE

Please provide the following information:

(a) State: GRENADA
(b) The official to be consulted regarding the responses to the questionnaire is:
( ) Mr.:
(✓) Ms.: Francia Noel
Title/position: IT Supervisor | Corporal of Police
Agency/office: Royal Grenada Police Force
Address: Police Headquarters, Fort George
St. George's, Grenada
Telephone number: 473-440-1666
Fax number: 473-440-4139
E-mail address: fnoel@rgpf.gd