

138

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

**1. LEGISLATION**

1.1 Has your country adopted laws to prevent, investigate, and punish cyber-crime? **Yes**

If so please list and enclose a copy preferably electronic of those laws: Please see copy attached

The Following types of Cyber-crime has been criminalized (Please see attached)

- **Illegal access**
- **Illegal interception**
- **Data interference**
- **System interference**
- **Misuse of devices**
- **Computer related forgery**
- **Computer related fraud**
- **Child pornography**
- **Offences related to infringements of copyright and related rights**

2. 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:

Offence	Person Charged	Court Results
Illegal Access	Yes	Pending
Misuse Device	Yes	Pending
Child Pornography	Yes	Pending
Computer Related Fraud	Yes	Pending
System interference	Yes	Guilty

3. If your country has not criminalized any of the above conduct please mention what steps if any, it has taken to do so: (They were criminalized)

4. Have your country adopted substantive or procedural legislation or any other necessary measures to enable it to obtain and preserve evidence in electronic form of any criminal offence? **Yes**

134

If so kindly provide a brief description of the previous and/or other measures in place in that regard together with a copy, preferably electronic thereof: Our Computer Misuse Act, Evidence and Procedure Code. Please see copies attached.

5. 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

If so kindly provide a brief description of the previous and/or other measures in place in that regard together with a copy, preferably electronic thereof: Our Computer Misuse Act, Evidence and Procedure Code. Please see copies attached.

6. 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 the possession or control which is stored in a computer system or a computer-data medium? Yes
- 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

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. Computer Misuse Act
- 2. Letter of request from the Commissioner of Police

Has your country adopted substantive or procedural legislation or the necessary measures whereby its competent authorities can?

- a) Seize, confiscate or attach computer systems or computer-data storage media? Yes
- b) Copy and keep the computer data accessed? Yes
- c) Maintain the integrity of the stored computer data? Yes
- d) Render inaccessible or remove the data in the accessed system? Yes

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. Computer Misuse Act.
- 2. Removable storages
- 3. Hard drive imaging
- 4. Utility Software

900 P

286

REGISTRATION

44300000/ P.008

185

3

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?

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.

SPECIALIZED UNITS

Has your country established specialized units or agencies specifically charged with the investigation and prosecution of computer crimes? Yes

If so, please supply the following information:

- Name of the unit or agency           **Cyber Crime Unit Royal Bahamas Police**
- Institution to which it reports:   **Royal Bahamas Police**
- Contact information                 **Royal Bahamas Police**
  - Name of contact                   **Assistant Superintendent Paul Rolle**
  - Address                               **Nassau Bahamas**
  - Telephone(s)                       **1-242-502-9986**
  - E-mail address                      **Paul@Criminalist.org**

Has your country established specialized units or agencies specifically charged with the investigation and prosecution of computer crimes? No

What measures 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?

- Investigation and prosecution are the same agency.
- Through good relations information is obtain with all the red tape, however the necessary document follows.

INTERNATIONAL COOPERATION

3.1 Has your country acceded to the council of Europe Convention on Cyber crime?

No

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

If so, please describe what that consideration has entailed:

3.2 Has your country joined the G8 24/7 High Tech Crimes Network? No



If not has your country taken any steps to join it? No

If so, please describe those steps:

Has your country adopted laws or other measures that enable processing of request for mutual assistance from other states which, in conformity with their domestic laws, have the power to investigate or prosecute computer crimes? Yes

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 Bahamas has a Mutual Legal Agreement Treaty (MLAT) with the United States of America, please see copies attached.

3.3 Has your country adopted laws or other measures that enable processing of request 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

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 Bahamas has a Mutual Legal Agreement Treaty (MLAT) with the United States of America, please see copies attached.

3.4 Has your government presented or received request 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

If so, please indicate the number of request presented and/ or received and the status of those requests: Unknown 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? 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? No

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

TOTAL P.007

2023192668

2023192668

189

5

**V Goals**

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

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:

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 it's ability to address crimes involving computers and the internet:

**INFORMATION ON THE OFFICIAL RESPONSIBLE FOR COMPLETION OF THIS QUESTIONNAIRE**

Please provide the following information:

(a) State: \_\_\_\_\_

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

( ) Mr.: \_\_\_\_\_

( ) Ms.: \_\_\_\_\_

Title/position: \_\_\_\_\_

Agency/ office: \_\_\_\_\_

Address: \_\_\_\_\_

Telephone number: \_\_\_\_\_

Fax number: \_\_\_\_\_

E-mail address: \_\_\_\_\_