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

OEA/Ser.K/XXXIV
CIBER-VIII/doc.1/13
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 ( )
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: A SCANNED COPY OF 18 U.S.C., SECTIONS 1030 AND 1037 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 (X) No ( )

If so, please list and enclose a copy, preferably electronic, of those laws: SEE, 18 U.S.C., SECTION 1030(b)

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

If so, please list and enclose a copy, preferably electronic, of those laws: SEE ATTACHED COPY OF 18 U.S.C., SECTION 2(a)

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: HOWEVER, CORPORATE CRIMINAL RESPONSIBILITY EXISTS/HAS DEVELOPED MOSTLY THROUGH CASE LAW (SEE, RETHINKING CORPORATE CRIMINAL LIABILITY, 82 IND. L.J. 411 (2007)).

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: _____

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 (X) 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: 18 U.S.C., SECTION 2703(F): "A SERVICE PROVIDER, UPON THE REQUEST OF A GOVERMENT ENTITY, SHALL TAKE ALL NECESSARY STEPS TO PRESERVE RECORDS... PENDING THE ISSUANCE OF A COURT ORDER."

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: SEIZURE AUTHORIZED BY LEGISLATION (RULE 41); IMAGING AUTHORIZED BY CASE LAW (SEE UNITED STATES V. VILAR, 2007 WL 1075041 (S.D.N.Y. APR. 4, 2007)).

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: 18 U.S.C. SECTION 2711(3)(A)(iii): "... ACTING ON A REQUEST FOR FOREIGN ASSISTANCE."

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: COUNTLESS REQUEST MADE AND RECEIVED.

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

3.2. 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: COMPUTER CRIME & INTELLECTUAL PROPERTY SECTION
- Institution to which it reports: U.S. DEPT. JUSTICE
- Internet address of the unit or agency: _____
- Contact information:
  - Name of contact: BETTY SHAVE
  - Address: WASHINGTON D.C.
  - Telephone(s): (202) 514-1026 Fax: (202) 514-6113
  - E-mail address: BETTY.SHAVE@USDOJ.GOV

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: WWW.JUSTICE.GOV/CRIMINAL/CYBERCRIME/DOCUMENTS.html

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: MANY SOURCES AVAILABLE INCLUDING: WWW.FBI.GOV/ABOUT-US/INVESTIGATE/CYBER

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: ____ COUNTLESS
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 ____ COUNTLESS
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 ( )

If so, please provide a detailed and specific description of the type of difficulties that have been encountered: _____

_____

_____

_____

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:

_____

_____

_____

_____

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: A NUMBER OF FEDERAL AND STATE LAW ENFORCEMENT AGENCIES OFFER TRAINING FOR THEIR STAFF

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: U.S. DEPT. OF JUSTICE CYBER-CRIME & INTELLECTUAL PROPERTY SECTION OFFER COURSES FOR FEDERAL & STATE PROSECUTORS

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: _____

INFORMATION ON THE OFFICIAL RESPONSIBLE FOR COMPLETION OF THIS QUESTIONNAIRE

Please provide the following information:

(a) State: UNITED STATES
(b) The official to be consulted regarding the responses to the questionnaire is:
( ) Mr.: RODOLFO ORJALES
( ) Ms.: _____
Title/position: SENIOR TRIAL ATTORNEY
Agency/office: U.S. DEPT. JUSTICE, COMPUTER CRIME SECTION
Address: WASHINGTON, D.C.
Telephone number: (202) 305 9321
Fax number: _____
E-mail address: RUDY.ORJALES@USDOJ.GOV