Organization of American States
Meetings of Ministers of Justice or of Ministers or Attorneys General of the Americas

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

RESPONSE OF THE UNITED STATES OF AMERICA

United States Department of Justice, Criminal Division
Computer Crime and Intellectual Property Section
December 11, 2009

I. LEGISLATION

1.1. The United States has the following cybercrime legislation in place[1]:

Substantive cyber-crime laws (e.g., laws prohibiting online identity theft, hacking, intrusion into computer systems, child pornography, intellectual property):

- 18 U.S.C. § 1028 – Fraud and related activity in connection with identification documents, authentication features, and information
- 18 U.S.C. § 1028A – Aggravated identity theft
- 18 U.S.C. § 1029 – Fraud and related activity in connection with access devices
- 18 U.S.C. § 1030 – Fraud and related activity in connection with computers
- 18 U.S.C. § 1037 – Fraud and related activity in connection with electronic mail
- 18 U.S.C. § 1343 – Fraud by wire, radio, or television
- 18 U.S.C. § 1362 – [Malicious mischief related to] Communications lines, stations, or systems
- 18 U.S.C. § 1462 – Importation or transportation of obscene matters
- 18 U.S.C. § 1465 – Transportation of obscene matters for sale or distribution

[1] The United States' federal criminal code is found generally at Title 18 of the United States Code (U.S.C.). However, some criminal offenses are found in other titles. Sections of the code are abbreviated: "18 U.S.C. § 1028" – the first number is the title and the second number is the section within the title.

All up-to-date statutes in electronic format are readily accessible at http://uscode.house.gov/; information about pending and recent legislation is provided at http://www.thomas.gov/.

- 18 U.S.C. § 1466A – Obscene visual representation of the sexual abuse of children
- 18 U.S.C. § 2251 – Sexual exploitation of children
- 18 U.S.C. § 2252 – Certain activities relating to material involving the sexual exploitation of minors
- 18 U.S.C. § 2252A – Certain activities relating to material constituting or containing child pornography
- 18 U.S.C. § 2252B – Misleading domain names on the Internet [to deceive minors]
- 18 U.S.C. § 2252C – Misleading words or digital images on the Internet
- 18 U.S.C. § 2425 – Use of interstate facilities to transmit information about a minor
- 18 U.S.C. § 2319 – Criminal infringement of a copyright
- 18 U.S.C. § 2511 – Unlawful interception and disclosure of wire, oral, or electronic communications
- 18 U.S.C. § 2701 – Unlawful access to stored communications
- 18 U.S.C. § 3121 – Unlawful use of pen register and trap and trace devices
- 17 U.S.C. § 506 – Criminal offenses [related to copyright]
- 47 U.S.C. § 605 — Unauthorized publication or use of communications
- 31 U.S.C. § 5366 – Criminal penalties [related to the prohibition on funding of unlawful Internet gambling]

As a result, the United States has criminalized the conduct listed in the questionnaire:

a) Illegal access,
b) Illegal interception,
c) Data interference,
d) System interference,
e) Misuse of devices,
f) Computer-related forgery,
g) Computer-related fraud,
h) Child pornography, and
i) Offenses related to infringements of copyright and related rights.

Every year, United States law enforcement entities investigate hundreds of cases involving the offenses listed above, many of which lead to prosecution by the United States Department of Justice. For example, between October 1, 2007 and September 30, 2008, 101 defendants were found guilty in United States federal courts of violating 18 U.S.C. § 1030, fraud and related activity in connection with computers.

Procedural cyber-crime laws (e.g., authority to preserve and obtain electronic data from third parties, including internet service providers; authority to intercept electronic communications; authority to search and seize electronic evidence):

- 18 U.S.C. §§ 2510-2522 – Interception of wire, oral, or electronic communication
- 18 U.S.C. §§ 2701-2712 – Preservation and disclosure of stored wire and electronic communication
- 18 U.S.C. §§ 3121-3127 – Pen registers and trap and trace devices [relating to recording of dialing, routing, addressing and signaling information]

1.2. Evidence in electronic form is admissible in the courts of the United States, pursuant to the federal Rules of Evidence[2].

1.3. The United States has legislation that enables competent authorities to order a third party, including an Internet service provider, to provide information stored in a computer system, subscriber information, and other records in its possession or control. This authority is found in 18 U.S.C. §§ 2701-2712, relating to stored wire and electronic communication; the federal Rules of Criminal Procedure[3]; and other laws and procedures of the United States.

1.4. The United States has legislation that enables competent authorities to:

a) Seize computer systems and computer data storage media,
b) Copy and keep computer data,
c) Maintain the integrity of stored computer data, and
d) Render inaccessible or remove data from an accessed system.

This authority is found in the federal Rules of Criminal Procedure[4], statutes governing civil and criminal forfeiture[5], and other laws and procedures of the United States.

The United States has legislation that permits competent authorities to intercept traffic and content data. This authority is found in 18 U.S.C. §§ 2510-2522, relating to interception of wire,

[2] Found at Title 28 Appendix, United States Code.
[3] Found at Title 18 Appendix, United States Code.
[4] Found at Title 18 Appendix, United States Code.
[5] Laws governing civil and criminal forfeiture are found in 18 U.S.C. § 981, 21 U.S.C. § 853, and other statutes.

oral, or electronic communication, and 18 U.S.C. §§ 3121-3127, relating to recording of dialing, routing, addressing and signaling information.

II. SPECIALIZED UNITS

2.1. The United States has entities specifically charged with the investigation and prosecution of computer crimes. The point of contact for these entities is:

> Computer Crime and Intellectual Property Section (CCIPS)
> Criminal Division, United States Department of Justice
> Address: 1301 New York Avenue NW, Suite 600, Washington DC, 20530
> Telephone: +1-202-514-1026, Fax: +1-202-514-6113

2.2. The United States has entities specifically charged with the prosecution of computer crimes. The point of contact for these entities is the Computer Crime and Intellectual Property Section, listed above.

2.3. The United States has adopted various measures 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. Public-private partnerships include:

- InfraGard. InfraGard is a partnership between the Federal Bureau of Investigation and the private sector. InfraGard is an association of businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to sharing information to protect critical infrastructure, including information technology infrastructure. See http://www.infragard.net/.

- The Internet Crime Complaint Center (IC3). The IC3 is a partnership between the Federal Bureau of Investigation and the National White Collar Crime Center, a private nonprofit organization, to serve as a means to receive Internet related criminal complaints and to further research, develop, and refer the criminal complaints to federal, state, local, or international law enforcement and/or regulatory agencies for any investigation they deem to be appropriate. See http://www.ic3.gov.

- The National Center for Missing & Exploited Children (NCMEC). The NCMEC's mission is to help prevent child abduction and sexual exploitation; help find missing children; and assist victims of child abduction and sexual exploitation, their families, and the professionals who serve them. NCMEC is a private, nonprofit organization that provides services nationwide for families and professionals in the prevention of abducted, endangered, and sexually exploited children. A significant part NCMEC's efforts relate to online exploitation of children. See http://www.missingkids.com.

III. INTERNATIONAL COOPERATION

3.1 The United States is a party to the Council of Europe Convention on Cybercrime. The convention entered into force for the United States on January 1, 2007.

3.2. The United States is a member of the G8 24/7 High Tech Crime Network.

3.3. The United States has laws and other measures that enable processing requests for mutual assistance from other states related to investigating and prosecuting computer crimes and for the purpose of obtaining electronic evidence. The three primary mechanisms for sharing electronic evidence are mutual legal assistance treaties, simultaneous criminal investigations involving a United States law enforcement agency and a foreign law enforcement agency, and letters rogatory.

In 2009, the United States enacted legislation to enhance the government's ability to process requests for mutual assistance. Amendments to 18 U.S.C. § 2703 and a new statute, 18 U.S.C. § 3512, relate to foreign requests for assistance in criminal investigations and prosecutions. This new law sets out clear authority and greater flexibility for United States prosecutors to obtain electronic and related evidence in response to foreign requests. The new law does not create a new mechanism for sharing evidence, but should improve the efficiency of existing procedures.

3.4 Each year, the United States receives and responds to hundreds of requests for mutual assistance for the investigation or prosecution of crimes related to computers and the internet.

IV. TRAINING

4.1. The United States provides a significant amount of training to law enforcement personnel on computer crimes and the collection of electronic evidence. All federal law enforcement agents receive such training during their initial law enforcement training and periodically throughout their careers. In addition, law enforcement personnel who specialize in computer crime and electronic evidence receive ongoing training in their areas of expertise.

Examples of training programs:

- Federal Law Enforcement Training Center (FLTC), Technical Operations Division, see http://www.fletc.gov/training/programs/technical-operations-division.

- Regional Computer Forensic Laboratory (RCFL), Training Portal, see http://www.rcfl.gov/index.cfm?fuseAction=Public.top2.

- Forward Edge Interactive Training and Resources to Combat Electronic Crime, see http://www.forwardedge2.com/.

4.2. The United States provides training to most prosecutors on computer crimes, the collection of electronic evidence, and use of electronic evidence in court. For example, the National Advocacy Center of the United States Department of Justice offers courses in basic cybercrimes, complex online crimes, computer forensics, and intellectual property crimes. See, http://www.justice.gov/usao/eousa/ole/index.html.

4.3. The United States' training goals are to ensure that all investigators and prosecutors have the basic knowledge and skills to collect and use electronic evidence, and that investigators and prosecutors who specialize in computer crimes are aware of the latest technologies and most up-to-date laws and methods for collecting electronic evidence.

4.4. The United States sends officials to all workshops presented by the Working Group on Cybercrime. These officials are responsible for the development and presentation of the workshops. In addition to providing instruction, federal prosecutors and investigators who attend the workshops gain a better understanding of the laws, capabilities, and efforts of all of the participating countries.

4.5. The workshops should focus on improved international cooperation in matters relating to electronic evidence, assisting member states to enact legislation consistent with the framework of the Council of Europe Convention on Cybercrime, and increasing the ability of member states to investigate and prosecute crimes involving computers and the Internet.

4.6. The Working Group on Cybercrime should remain the leader within the OAS on cybercrime and electronic evidence matters, encourage improved international cooperation among member states and with states worldwide, and identify resources within the OAS and member states to improve member states' ability to investigate and prosecute crimes involving computers and the Internet.

The United States' response was prepared by:

Albert Rees
Trial Attorney
Computer Crime and Intellectual Property Section
Criminal Division, United States Department of Justice
Address: 1301 New York Avenue NW, Suite 600, Washington DC 20530
Tel: +1-202-514-1026
Fax: +1-202-514-6113
Email: albert.rees@usdoj.gov
Website: http://www.cybercrime.gov