Request for Disclosure of Registrant Information for Law Enforcement and National Security Agencies - Rules and Procedures
Version 1.5 (May 20, 2015)

Background

These Rules and Procedures are implemented pursuant to CIRA's *Privacy Policy*, to provide the process for certain law enforcement and national security agencies to request the disclosure, under certain limited and specified circumstances, of certain specific information of Registrants that is not publicly available through CIRA's WHOIS search tool.

Except as expressly specified herein or in the Policy, any other request for disclosure of information of Individual Registrants must be by way of an order, ruling, decision, subpoena, warrant, or judgment.

These Rules and Procedures outline:

- What specific information of Registrants may be disclosed under these Rules and Procedures, pursuant to a request for disclosure;
- Who may request such information be disclosed by CIRA, pursuant to these Rules and Procedures (" Law Enforcement Requestors"); and
- What express requirements the Law Enforcement Requestors must meet, before CIRA will consider disclosure of information, pursuant to a request.

All capitalized terms used herein but not defined, shall the meanings as set out in CIRA's *Registrant Agreement* or *Registrar Agreement*.

Rules and Procedures

1. Information Subject to Disclosure.

   These Rules and Procedures provide for the potential disclosure of the following information of Registrants, as found in the CIRA Registry:

   a. The name of the Registrant;
   b. The name of the Registrant's Administrative Contact and Technical Contact; and
   c. The postal address and email address of the Administrative Contact and Technical Contact.

   (collectively, "Information").

   CIRA will not disclose any other information under these Rules and Procedures.

2. Who May Request Disclosure of Information. Law Enforcement Requestors must be a member of a Canadian law enforcement or national security agency that is a government institution or part of a government institution, who has identified its lawful authority to obtain the Information, and who complies with all of the obligations of Section 3 below.

3. Requirements. To be able to request Information, a Law Enforcement Requestor must meet **all** of the following requirements:

a) The Information is not publicly available through CIRA's WHOIS search tool.

b) The Law Enforcement Requestor must require the Information for the purpose of either:

i. Enforcing a Child Exploitation Law of Canada (as defined in Schedule A hereto) or carrying out an investigation relating to the enforcement of such Child Exploitation Law. For purposes of these Rules and Procedures, "Child Exploitation Law" has the meaning set forth in Schedule A hereto;

or

ii. Investigating:
(a) an Espionage or Sabotage Threat; or
(b) a Terrorist Threat, as defined in Schedule "A" attached hereto

or

iii. Investigating an actual, or serious and imminent, threat to the stability or integrity of the Internet, resulting from:

(a) a Denial of Service Attack that originates from a CIRA domain;
(b) Malicious Hacking that originates from a CIRA domain;
(c) Phishing originating from a CIRA domain; or
(d) Pharming originating from a CIRA domain.

(as such terms are defined in Schedule "A" attached hereto)

(Collectively, a "Law Enforcement Matter"). Nothing else shall constitute a Law Enforcement Matter hereunder.

c) The Law Enforcement Requestor must be requesting the Information for the sole purpose of the Law Enforcement Matter, and the Information, if provided, may not be used (in whole or in part) for any other reason.

d) The request for the Information of the Registrant must be in the applicable form as specified by CIRA from time to time. The form must be: (i) accurately and fully completed; (ii) signed by the Law Enforcement Requestor or their appointed representative, certifying full compliance with the requirements of these Rules and Procedures and that the information in the form is truthful and correct; and (iii) the original sent by postal mail, courier, email, facsimile or delivered in person to the address specified below:

Disclosure Requests
Canadian Internet Registration Authority
319 McRae Avenue, Suite 700
Ottawa, Ontario
K1Z 0B9
Facsimile: (613) 237-0534 or 1-800-285-0517
Email: disclosurerequests@cira.ca

4. CIRA Response. CIRA will respond to the request as quickly as possible after receipt of a form. CIRA reserves the right not to respond to a request, or to refuse a request where the Law Enforcement Requestor did not, or CIRA believes may not, fully comply with all of the requirements of these Rules and Procedures.

5. Notice to Registrant. If CIRA approves a request hereunder, CIRA shall, unless prohibited by law, not less than 30 and not more than 60 days after disclosure of the Information, use reasonable efforts to send an email to the Administrative Contact of the Registrant indicating: (a) that CIRA has disclosed the Information; and (b) the name of the Law Enforcement or National Security Agency to whom CIRA has disclosed the Information.

Schedule A

Definitions

For purposes of these Rules and Procedures:

"Child Exploitation Law" means the following offences in the Criminal Code:

(a) Those offences that are listed in the definition of "designated offence" in s. 490.011; and

(b) Sections: 159 (Anal Intercourse), 160(2) (Bestiality), 162 (Voyeurism), 282 (Abduction contra custody), and 283 (Abduction),

in each case where the victim of such offence is a person under 18.

"Denial of Service Attack" means an attempt to make an Internet site or Internet service unavailable to its intended users by overwhelming that site or service with service requests, and includes a distributed denial-of-service attack (DDoS attack).

"Espionage or Sabotage Threat" means espionage or sabotage that is against Canada or is detrimental to the interests of Canada or activities directed toward or in support of such espionage or sabotage.

"Malicious Hacking" means the intentional and unauthorized access to a computer system.

"Phishing" means an attempt to acquire sensitive information (such as usernames, passwords, and credit card details) by masquerading as a trustworthy entity in an electronic communication.

"Pharming" means an attempt to redirect an Internet site or Internet service to a fake site or service without the end user's knowledge.

"Terrorist Threat" means activities within or relating to Canada directed toward or in support of the threat or use of acts of serious violence against persons or property for the purpose of achieving a political, religious or ideological objective within Canada or a foreign state.