Governmental Advisory Committee
Chairman

ICANN

Mr. Peter Dengate Thrush
Chairman of the Board
ICANN

Paris, 12 April 2010

Re: LEA RAA Amendment/Due Diligence Proposals

Dear Peter,

As per the GAC Nairobi Communiqué, I am very pleased to forward statements of support for the "Law Enforcement Due Diligence Recommendations for ICANN" proposals developed by law enforcement agencies from Australia, Canada, New Zealand, the UK and the U.S. for due diligence on accredited registrars and amendments to the Registrar Accreditation Agreement (RAA) from the Interpol Working Party on IT Crime-Europe and the G8 Lyon-Roma Group's High Tech Crime Subgroup. As you will recall, the law enforcement proposals were shared with the GAC, the ICANN Board and broader ICANN community, including the RAA Working Group under the Generic Names Supporting Organization (GNSO), during the October 2009 ICANN meeting in Seoul, Korea.

Also attached are recommendations developed by the participants in the Council of Europe (COE) Octopus Interface Conference, held March 23-25, 2010 as part of the COE Project on Cybercrime. These recommendations include a specific reference the law enforcement proposals noted above. It is notable that all three documents urge ICANN to implement the law enforcement recommendations.

The GNSO Council Chair, Chuck Gomes, is copied on this letter to ensure that the attached statements are circulated to the GNSO RAA Working Group. The GAC expects that these proposals, and the attached statements of support, will be thoroughly examined and taken into consideration by ICANN.

I anticipate that many GAC members will be joined by their law enforcement colleagues from capitals at the Brussels meeting in June 2010, and have no doubt that those law enforcement representatives present at the Brussels meeting will make themselves available to discuss their proposals further and to answer any outstanding questions.

Yours sincerely

Janis Karklins
Chairman of the Governmental Advisory Committee,
Ambassador of Latvia to France

Cc: Mr. Chuck Gomes, GNSO Council Chair

Attachments:
Interpol Working Party on IT Crime-Europe Statement
G8 Lyon-Roma Group High Tech Crime Subgroup Statement
Council of Europe Project on Cybercrime, "Messages from the Octopus Conference"

ICANN Governmental Advisory Committee; GAC Secretariat
1016, Electronics Niketan, 6 CGO Complex, Lodi Road, New Delhi, – 110 003, India
Telephone: +91 11 2430 1116. *Fax*: +91 11 2436 3126 *E-mail*: gacsec@gac.icann.org
Website: http://www.gac.icann.org

International Criminal Police Organization
Organización Internacional de Policía Criminal

Organisation internationale de police criminelle
المنظمة الدولية للشرطة الجنائية

200, quai Charles de Gaulle
69006 LYON - FRANCE
Telephone : +33 4 72 44 70 00
Facsimile : + 33 4 72 44 71 63
http://www.interpol.int

INTERPOL

General Secretariat
Secrétariat général
Secretaría General
الأمانة العامة

26 March 2010

Subject:
Law Enforcement Due Diligence Recommendations for ICANN

In October 2009, a series of recommendations for amendments to ICANN's Registrar Accreditation Agreement (RAA) was proposed to ICANN by law enforcement agencies from the US, UK, Canada, Australia and New Zealand.

The principle aim of these proposals is to implement stronger controls around domain name registration and to ensure a mandatory and rigorous regulatory framework to govern ICANN's contracts with domain registrars. They include requirements for effective due diligence on accredited registrars, controls to ensure more accurate WHOIS information and availability for Law Enforcement, in addition to improved transparency around domain name resellers and third party beneficiaries.

The recommendations are considered to be necessary to aid the prevention and disruption of efforts to exploit domain registration procedures for criminal purposes. The international law enforcement community views these recommendations as vital in preventing crimes involving the Domain Name System.

The Interpol Working Party on IT Crime - Europe, which comprises representatives from law enforcement bodies of 15 European countries, is in support of these recommendations and recommends their implementation.

Wolfgang Schreiber
Chairperson
Interpol Working Party
on IT Crime – Europe

G8 Lyon-Roma Group

High Tech Crime Subgroup

In October 2009, a series of recommendations for amendments to ICANN's Registrar Accreditation Agreement (RAA) was proposed to ICANN by law enforcement agencies from the US, UK, Canada, Australia and New Zealand.

The principle aim of these proposals is to implement stronger controls around domain name registration and to ensure a mandatory and rigorous regulatory framework to govern ICANN's contracts with domain registrars. They include requirements for effective due diligence on accredited registrars, controls to ensure more accurate WHOIS information and availability for Law Enforcement, in addition to improved transparency around domain name resellers and third party beneficiaries.

The recommendations are considered to be necessary to aid the prevention and disruption of efforts to exploit domain registration procedures for criminal purposes. The international law enforcement community views these recommendations as vital in preventing crimes involving the Domain Name System.

The G8 High Technology Crime Subgroup (HTCSG), which comprises representatives from law enforcement, justice departments and other governmental bodies of the G8 countries, is in support of these recommendations and recommends their implementation.

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Octopus Interface conference
Cooperation against cybercrime
23 – 25 March 2010
Council of Europe, Strasbourg, France

25 March 10/provisional

Messages from the Octopus conference

More than 300 cybercrime experts representing countries from all continents, international organisations and the private sector met at the Council of Europe in Strasbourg from 23 to 25 March 2010 to enhance their cooperation against cybercrime. At the close of the conference participants adopted key messages aimed a guiding further action.

Participants share a common interest in pursuing the most effective approaches against the growing threat of cybercrime that societies worldwide are faced with.

Effective approaches against cybercrime comprise a wide range of innovative initiatives and actions that need to be pursued in a dynamic and pragmatic manner by public and private sector stakeholders.

At the same time, measures against cybercrime are a shared responsibility and should be based on a set of common principles to allow for clear guidance to governments and organisations, to facilitate partnerships and to ensure the political commitment to cooperate.

In this connection, participants in the conference underline that:

- For security and the protection of rights to reinforce each other, measures against cybercrime must follow principles of human rights and the rule of law.
- Security and the protection of rights is the responsibility of both public authorities and private sector organisations.
- Broadest possible implementation of existing tools and instruments will have the most effective impact on cybercrime in the most efficient manner.

Following detailed discussions, participants recommend:

- Making decision makers aware of the risks of cybercrime and encouraging them to exercise their responsibility. Indicators of political commitment include steps towards the adoption of legislation and institution building, effective international cooperation and allocation of the necessary resources.
- Implementation of the Budapest Convention on Cybercrime worldwide to sustain legislative reforms already underway in a large number of countries. Countries should consider becoming parties to make use of the international cooperation provisions of this treaty. Consensus on this treaty as a common framework of reference helps mobilise resources and create partnerships among public and private sector organisations. In this connection, the ratification of the Budapest Convention by Azerbaijan, Montenegro and Portugal prior and during the conference, and the expression of interest to accede by Argentina and other countries serve as examples to other countries.
- Establishing the Budapest Convention as the global standard goes hand in hand with strengthening the Cybercrime Convention Committee (T-CY) as a forum for information-sharing network, policy-making and standard-setting. It is encouraged to address issues

not (exhaustively) regulated by the provisions of the Cybercrime Convention such as electronic evidence, jurisdiction and liability of ISP's.
- Coherent and systematic training of law enforcement, prosecutors and judges based on good practices, concepts and materials already available.
- The establishment and strengthening of high-tech crime and cybercrime units, and incidents response and reporting teams and systems.
- The development of cooperation procedures between law enforcement agencies, CERTs/CSIRTs as well as internet service providers and the IT industry.
- Due diligence by ICANN, registrars and registries and accurate WHOIS information. Endorsement of the "Law Enforcement Recommended Amendments to ICANN's Registrar Accreditation Agreement (RAA) and Due Diligence Recommendations" in line with data protection standards. ICANN is encouraged to implement these recommendations without delay.
- The many networks and initiatives against cybercrime that exist already create a dynamic and innovative environment involving a wide range of actors. Stronger networking among networks is encouraged to allow for synergies and reduce duplication. The mapping of networks exercise initiated by the Council of Europe should be continued.
- A contact list for enhanced cooperation between industry and law enforcement should be established. A proposal for a secure portal for interest parties is in preparation.
- Initiatives aimed at preventing, protecting and prosecuting the sexual exploitation and abuse of children are most valuable but require stronger support and consistency. The "Lanzarote" Convention of the Council of Europe (CETS 201) offers guidance in this respect and provides benchmarks to determine progress.
- Making use of the guidelines for law enforcement – ISP cooperation adopted at the Octopus Conference in 2008.
- Completion and broad dissemination of the results by the Council of Europe of the typology study on criminal money flows on the Internet that is currently underway.
- In order to meet the law enforcement and privacy challenges related to cloud computing existing instruments on international cooperation – such as the Data Protection Convention (CETS 108) and the Budapest Convention – need to be applied more widely and efficiently. Additional international standards on law enforcement access to data stored in the "clouds" may need to be considered. Globally trusted privacy and data protection standards and policies addressing those issues need to be put in place and the Council of Europe is encouraged to continue addressing these issues in its standard-setting activities as well as by the Global Project on Cybercrime.

Public authorities, international organisations, civil society (including non-governmental organisations) and the private sector should apply existing tools and instrument without delay and cooperate with each other to identify additional measures and responses to emerging threats and challenges.

In order to add impetus and resources to efforts against cybercrime and allow societies worldwide to make best possible use of tools, instruments, good practices and initiatives already available, a global action plan aimed at obtaining a clear picture of criminal justice capacities and pressing needs, mobilising resources and providing support, and assessing progress made should be launched, preferably by the United Nations and the Council of Europe in partnership with the European Union, Parties to the Budapest Convention, and other interested parties.

The results of the Octopus conference should be submitted to the United Nations Crime Congress in Salvador, Brazil (12-19 April 2010) for consideration.