Comments of Coalition for Online Accountability (COA)

Re "Draft Development Program Snapshot/ High Security Zone TLD Advisory Group"

April 8, 2010

The Coalition for Online Accountability (COA) appreciates this opportunity to comment on the above-referenced document ("Snapshot"). See http://www.icann.org/en/public-comment/#hstld.

COA consists of eight leading copyright industry companies, trade associations and member organizations of copyright owners. These are the American Society of Composers, Authors and Publishers (ASCAP); Broadcast Music, Inc. (BMI); the Entertainment Software Association (ESA); the Motion Picture Association of America (MPAA); the Recording Industry Association of America (RIAA); the Software and Information Industry Association (SIIA); Time Warner Inc.; and the Walt Disney Company. COA has participated actively, both as a member of the Intellectual Property Constituency and in its own behalf, in all aspects of the new gTLD program. Specifically, COA provided its views on the High Security Zone TLD (HSTLD) concept on November 22, 2009, in its comments on an ICANN background paper on "Mitigating Malicious Conduct" in the new gTLDs. See http://www.onlineaccountability.net/pdf/2009_Nov22_COA_comments_on_malicious_conduct_paper.pdf

The "Snapshot" does not address the most significant issue raised by broad segments of the community when ICANN floated the HSTLD concept some seven months ago. This issue can be encapsulated as follows:

- *If strong protections against malicious conduct in the operation of new gTLD registries are in the interests of all parties, and of the public at large, why does ICANN insist that these protections can only be adopted as a purely voluntary program?*

- *Why are new gTLD applicants not required to meet these stronger standards – or at least provided strong incentives to do so (such as a point credit in the evaluation process) ?*

- *At a minimum, why should such requirements or incentives not be provided for a defined set of proposed new gTLDs that present unusually high risks of providing a venue for criminal, fraudulent or illegal conduct?*

The "Snapshot" sunnily reports (Section 1.0) that "much of the community response to the [HSTLD] concept paper was positive." But many commenters, reflecting a range of perspectives, raised precisely the concern summarized above. According to ICANN's own summary of comments received, objections to a purely voluntary HSTLD program were raised by, among others, Time Warner Inc.; BITS/Financial Services Roundtable; Software and Information Industry Association; Microsoft; Intellectual Property Constituency of GNSO; American Bankers Association; International Trademark Association; and Internet Identity. See

http://www.icann.org/en/topics/new-gtlds/summary-analysis-agv3-15feb10-en.pdf, page 34 et seq..[1] The "Snapshot" does not respond to this concern in any way.

COA recognizes that the Advisory Group which took the "Snapshot" is limited to development of "the voluntary HSTLD concept material originally published" by ICANN staff. (Section 2.0) But a review of the "Snapshot" document demonstrates that the issue of requirements or incentives to adopt such a program is inescapable.

For instance, in a "problem statement" adopted by the Advisory Group, it is noted that higher standards are in the interests of "end-users," which apparently refers to the billions of Internet users to whom new gTLDs would be directed. As section 2.5 of the "Snapshot" states:

"End-Users would like to know that when they type in a given domain name, or navigate from a bookmark, etc. that they go to the right domain, and that the DNS, etc. hasn't been hijacked. "

If a feasible means to reduce the risk of this malicious abuse can be identified, why should not new gTLD applicants be required – or at least provided strong incentives – to adopt it? Why should adoption remain a purely voluntary decision that provides an applicant with no benefit in the evaluation process? Which end-users do not deserve this protection?

Similarly, the "problem statement" continues:

" End-Users would like to understand that a domain name registered within a particular gTLD is subject to registration standards, policies and procedures that are aimed at reducing malicious conduct by such registrants."

Isn't this a legitimate expectation for users of all new gTLDs? Why should the adoption of such "standards, policies and procedures" against malicious conduct by registrants be purely voluntary on the part of new registry applicants? Shouldn't requirements or strong incentives be applied, at least where the risk of such malicious conduct is especially great? Which end-users do not deserve this protection?

Thus far, ICANN's only formal response to the widespread concern about leaving the HSTLD program purely voluntary, with no evaluation-based incentives for adoption by any new gTLD applicant, is as follows:

"Although the HSTLD program is still under development (current published documents are concept or development only), it is currently anticipated that the resulting standards created by the HSTLD program will be voluntary in nature. This position may be subject to change, as

[1] ICANN's summary also asserts that "the HSTLD program was strongly supported by international law enforcement during ICANN's most recent global meeting in Seoul Korea in the session on DNS abuse (http://sel.icann.org/node/6961). " See http://www.icann.org/en/topics/new-gtlds/summary-analysis-agv3-15feb10-en.pdf, page 42. But the only relevant statement from a law enforcement official at that session was that "certainly the developments of the high-security zone verification program and the added checks within that are most welcome." We doubt that law enforcement officials embrace the concept of a purely voluntary HSTLD program, with no requirements or incentives, and urge ICANN to clarify the law enforcement position.

the ICANN community will ultimately decide the overall course of the HSTLD program, including the voluntary or mandatory nature of the program. This position will be established through a multi-stakeholder process."

http://www.icann.org/en/topics/new-gtlds/summary-analysis-agv3-15feb10-en.pdf, at 40.

It is past time for ICANN to spell out when that "multi-stakeholder process" will begin, how it will be carried out, and how the organization's commitment under the Affirmation of Commitments to make decisions "in the public interest" will be reflected. The "Snapshot" does not even attempt to address these critical issues. Until ICANN decides to grapple with this question, it will scarcely have begun (much less completed) the task of resolving the "overarching issue" of malicious conduct in the new gTLDs; and accordingly it will remain far from ready to open the application window for new gTLDs.

COA looks forward to the opportunity to present in more detail its views that:

- Strengthened protections against malicious conduct should be required for at least a defined set of new gTLDs, including those at an unusually high risk of being the venue for criminal, fraudulent, or illegal conduct, including but not limited to copyright piracy. COA reiterates (from its November 2009 comments) its readiness to work with ICANN staff to fashion a workable definition for this subset of new gTLDs.

- Given the ICANN staff's aversion to any process that will require the recognition or definition of any category of new gTLD applications that ought to be subject to different evaluation standards, shouldn't the one category that is already recognized – community applications – be required to meet heightened security standards in order to protect their registrants and the community that they claim to serve?

- Whatever approach ICANN ultimately decides to take with regard to the HSTLD concept, it is essential that it provide some mechanism for some party to challenge a particular gTLD application on the grounds that it offers insufficient protections against malicious conduct.

Respectfully submitted,

Steven J. Metalitz, counsel to COA

Mitchell Silberberg & Knupp LLP | 1818 N Street, N.W., 8th Floor, Washington, D.C. 20036 USA | tel: (+1) 202 355-7902| fax: (+1) 202 355-7899| met@msk.com