# HIGH SECURITY TOP LEVEL DOMAIN-DRAFT PROGRAM DEVELOPMENT SNAPSHOT
# (16 June – 21 July 2010)

Source: The text of the comments may be found at http://forum.icann.org/lists/hstld-program-snapshot/.

## KEY POINTS

- The HSTLD program criteria and controls have been developed by the community-led High Security TLD Advisory Group (HSTLD AG).
- The current position of the HSTLD program is that if it's deemed viable to implement, it will be voluntary in nature and operated by an independent third party outside of ICANN.
- Comments gathered through this comment period will be taken into account during ongoing development of the HSTLD program.

## SUMMARY OF COMMENTS

ICANN does not value public input

We will passively resist by not participating in a process that only leads to predetermined outcomes. We request that ICANN notify the community when it is ready and willing to demonstrate that it properly values public comments. *G. Kirikos (20 July 2010).*

Mandatory baseline for registries

The main problem is the voluntary nature of many of the key safeguards that ICANN has proposed to deal with malicious conduct. At a minimum, ICANN should require registry operators of new gTLDs to implement basic procedures to help prevent, or to expedite response to, malicious conduct involving registrations that they sponsor. *Time Warner (21 July 2010).*

Support for malicious conduct recommendations but outcome still unclear

There have been no fundamental changes in the approach ICANN is taking to this critical issue. With respect to the update paper and the nine recommendations from which controls for reducing the potential for malicious conduct within gTLDs could be created, no timetable is provided in most cases for the next steps—e.g., on the SSAC working group report on removal of orphan glue records. COA supports the first eight recommendations but it is too early to say if taken as a whole they would reduce the potential for malicious conduct to a satisfactory degree. *COA (21 July 2010).*

Draft framework for high security zones verification—incentives needed

The ninth recommendation seems far from implementation—there is no timetable. COA is concerned that this framework, even when made actionable, will contribute little or nothing to reducing malicious conduct because it is completely voluntary and lacks incentives within the application process for any gTLD applicant to adopt any part of it. Possible methods to address this include:

- Option 1—Mandatory As COA already called for previously, make mandatory the High Security Zones Verification Program either for all new TLDs or at least for a defined set of new TLDs that require a "high-confidence infrastructure" or that are determined to be at an unusually high risk of being the venue for criminal, fraudulent or illegal conduct (e.g., copyright piracy). ICANN staff has not responded to COA's offer to work with ICANN to develop a workable definition of this subset of new gTLDs. *COA (21 July 2010).*

- Option 2—Incentives through extra points Also pointed out by COA previously, applicants could have incentives to adopt these enhanced protections against malicious conduct by getting extra points in the evaluation process for adopting the protections, or through deducting some points from applicants who failed to meet these standards. *COA (21 July 2010).*

- Option 3—Objections A third method COA has previously suggested is to give someone the role of objecting to any application for which, by its nature, failure to provide enhanced protections would inappropriately expose some segment of the public to an unacceptable risk of harm. This option is less desirable in some ways since it would delay to a later point in the process the elimination of new gTLD applications that carry with them excessive risk. *COA (21 July 2010).*

ICANN staff response requested
COA seeks a meaningful response from ICANN staff to all three options. Until such a response is provided, it is impossible to consider the "malicious behavior" issue satisfactorily resolved, or even to state a realistic timetable for doing so. *COA (21 July 2010).*

Classify the program as voluntary and let consumers decide
This program deserves support, but its real value to consumers will not be known until after it is operational. Therefore, I strongly believe it should be voluntary so that consumers in the marketplace can make their own assessment of the program's worth and choose between high security TLDs and other TLDs. If there is real consumer value in the program, then market forces will drive its broader adoption. *R. Tindal (21 July 2010).*

The program should be voluntary
Consistent with the almost uniform view of the Working Group, the program should be voluntary—i.e., it might be appropriate for some TLDs and not others, or it might be appropriate for one use of a TLD of the same name and not another. One size does not fit all and some TLDs would not warrant the additional expense associated with making the program mandatory. If TLDs that are part of the program are more successful marketing this feature in the marketplace, then more TLDs will want to join as well. That choice should be left to consumers. *J. Nevett (22 July 2010).*

**ANALYSIS AND PROPOSED POSITION**

In general, comments suggested that the HSTLD program should be voluntary and that if there is perceived value in it, the marketplace will evolve to accommodate the demand. The HSTLD program is currently being explored and its viability is under review and

consideration. On 22 September 2010, ICANN in coordination with its HSTLD AG issued a Request for Information (RFI) on the HSTLD Program. The purpose of the RFI is to assist the ICANN community in understanding potential frameworks and approaches for evaluating TLD registries against the HSTLD criteria, determine where improvements to draft criteria and the overall program may be necessary to ensure its success, and to assess the viability of the proposed HSTLD Program.

One commenter suggested the program should be mandatory for TLDs that require "high-confidence infrastructure" or that are determined to have an unusually high risk of being the venue for criminal, fraudulent or illegal conduct. Another commenter suggested that applicants could be incented to adopt enhanced protections against malicious conduct by either getting extra points or through deducting points in the evaluation process.

The COA made three comments meriting a specific response. The comments were well thought out and although the responses below indicate that the suggestions cannot be implemented at this time – they should be considered when the HSTLD program, or one similar to it, is ready to launch.

Option1 – COA offered to work with ICANN to develop a workable definition of a subset of new gTLDs that require a "high-confidence infrastructure" or that are determined to be at an unusually high risk of being the venue for criminal, fraudulent or illegal conduct. *(Response: As work on the HSTLD designation progresses, ICANN welcomes the support of the community, including the COA, to investigate such a process. Some work has been done – see the public letter by BITS describing definitions of entities that provide financial services.)*

Option 2 - COA suggested that applicants could have incentives to adopt enhanced protections against malicious conduct by getting extra points in the evaluation process for adopting the protections, or through deducting some points from applicants who failed to meet these standards.
*(Response: As the HSTLD validation would be voluntary and operated by an independent third party, awarding or deducting points during the evaluation process based upon a commitment in the application could be a means for applicants to game the process, without careful management. An option for consideration for adoption of high security measures has been introduced into the scoring criteria. For the point system to be adjusted in some more definite way, the criteria and program would have to be certain.)*

Option 3 - COA suggested that someone should be given the role of objecting to any application for which, by its nature, failure to provide enhanced protections would inappropriately expose some segment of the public to an unacceptable risk of harm. *(Response: The new gTLD program provides for a community objection process that is detailed in Section 3.1 of Module 3 of Applicant Guidebook v4 that may be useful. In addition, the Independent Objector has the role of acting in the best interests of the public and has standing to object to applications on community grounds where this is deemed appropriate*).

There have been some changes to the Guidebook in anticipation of this type of high-security designation.

### NEXT STEPS WITH HSTLD PROGRAM

ICANN and the HSTLD AG agreed there is value in conducting a RFI on the program, and as noted above it was published on 22 September 2010. After the RFI period closes on 23 November 2010 and ICANN and the HSTLD AG have had adequate time to respond to questions and to summarize and analyze the responses, a determination about next steps will be made.

ICANN remains committed to mitigating malicious conduct in new gTLDs and supports the development of the HSTLD concept as a voluntary, independently operated program. Some in the community have taken ICANN Board Resolution 2.8 Mitigating Malicious Conduct[1] as a lack of support for the concept. While the Board said it will not be signing on to be the operator of such a product, it does support its concept just as it has other measures (e.g., URS, prohibition of wildcarding, centralized zone file access, etc.) to mitigate malicious conduct in new gTLDs.

## RESPONDENTS

George Kirikos (G. Kirikos)
Time Warner Inc. (Time Warner)
Coalition for Online Accountability (COA)
Richard Tindal (R. Tindal)
Jon Nevett (J. Nevett)

[1] Board Resolution is viewable at http://icann.org/en/minutes/resolutions-25sep10-en.htm#2.8.