[D R A F T 4.13.10]

HIGH SECURITY TOP LEVEL DOMAIN-DRAFT PROGRAM DEVELOPMENT SNAPSHOT
(22 Feb.-8 April 2010)

Source: The text of the comments may be found at http://forum.icann.org/lists/hstld-snapshot-15feb10/. The transcript text (Nairobi meeting) may be found at http://nbo.icann.org/node/8875.

KEY POINTS

- The HSTLD program is under development by a stake holder working group, the High Security TLD Advisory Group (HSTLD AG).
- The current overall position of the HSTLD program is that the program will be voluntary in nature, although this is subject to change, as the ICANN community, through a multi-stakeholder, consensus based process, considers the HSTLD program.
- Comments gathered through this comment period will be taken into account during the development of the HSTLD program.

SUMMARY OF COMMENTS

Modifications needed. The INTA Internet Committee applauds the efforts of the HSTLD Advisory Group but believes that the overarching issue of malicious conduct in new gTLDs will not be addressed unless the HSTLD program is modified, a level of mandatory participation in the program is required, and the Draft Applicant Guidebook is further revised to address the comments and concerns raised by the community. *INTA Internet Committee (8 April 2010).*

Snapshot does not address the most significant issue. The snapshot does not respond to the objection raised by a number of parties to a purely voluntary HSTLD program. 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 pure voluntary program? Why are the 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? *COA (8 April 2010).*

Voluntary framework open to innovation.
Go Daddy supports the concept of a voluntary, high security framework for new gTLD zones with the security responsibilities within the zone shared and coordinated by the registry, participating registrars and registrants. Go Daddy has numerous concerns about any “top down” centralized attempts to foster such high security zones. The most effective HSTLD is one that is open to innovation, valued by its intended end users, and

widely adopted as necessary for conducting commerce within that specific HSTLD. *Go Daddy (9 April 2010).*

A better balance must be struck between real security issues and market forces, e.g., allowing potential registrants to decide whether to use a certain HSTLD (possibly based on audits and certifications it has obtained, insurance statements, imprimatur from government, or other reputational endorsements) but not because it is mandated by ICANN. *D. Smiley (10 Mar. 2010).*

Outside of ICANN mission and core responsibilities.
The HSTLD concept lies outside of ICANN's core mission and responsibilities. ICANN's commitments to transparency and consensus policy development are, in many respects, incompatible with effective abuse mitigation and broader security efforts. ICANN should serve primarily a coordinating role in bringing together the interested and necessary parties to develop the program, and no role in its administration or enforcement. *Go Daddy (9 April 2010).*

Developing high security zones for particular gTLDs is not an appropriate role for ICANN because: (1) it is not within ICANN's limited technical coordination mission related to Internet identifiers; (2) it would expand ICANN's authority to address malicious uses of domain names; (3) it would put ICANN into direct competition with organizations that already are capable of performing such a function; and (4) the demand for such zones could be met more effectively by registries in cooperation with existing security organizations. *RySG (8 April 2010).*

Consideration of alternatives.
In its development of a detailed, prescriptive program for HSTLDs, ICANN may be selecting a preferred model at the expense of more effective alternatives. DNS is not unique to TLD zones. Equivalent programs may benefit high-security hosting providers, ISPs and payment processors as well. A better approach may be to specify more abstract "rules of the road" for a HSTLD and allow applicants and service providers to innovate and collaborate within this basic framework. *Go Daddy (9 April 2010).*

It is important to be realistic about the role the DNS has in the overall Internet ecosystem. A "seal" is not that important and should not end up being perceived as an ICANN profit center. The proposal seems to err on the side of over-regulation, not taking into account free market principles. ICANN should make sure to fully consider the views from the businesses and entrepreneurs that will turn the HSTLD + DNSSEC combination into a platform for innovation and international cooperation in cyber security so everyone can benefit, instead of a playground for policy/technical/regulatory elites to run amok. *D. Smiley (10 Mar. 2010).*

Standards development.
The draft program has ICANN too involved in developing new standards and certifications for IT security, data integrity, procedure quality and overall business operations. The efforts and costs required for these programs could dramatically increase ICANN's size and scope and are unnecessary given the abundance of viable alternatives such as ISO 17799, ISO/IEC 27001, PCI-DSS, and others. A better approach is for ICANN to provide a platform to bring together interested gTLD applicants and operators to collaborate with existing standards bodies and others in the industry to

develop the HSTLD framework incorporating appropriate standards and programs already governing a given topic, practice, or business function. *Go Daddy (9 April 2010).*

The extent of ICANN's participation in the development of the proposed self-certification program is unclear and without foundation. The development of the standards should be left to other organizations that have the appropriate expertise in this area. *RySG (8 April 2010).*

Opposition to self-certification and report card approach. The INTA Internet Committee cautions against a self-certification or report card program because of its inherent lack of transparency and controls. The report card concept is too complex to be useful and self-auditing will undermine the usefulness of HSTLDs. The name "high security" implies something more than self-auditing, which may or may not be performed in a diligent manner, and may open the door for some registries to cut corners. Therefore, regular, independent certification is essential to the credibility of HSTLDs. *INTA Internet Committee (8 April 2010).*

HSTLD not a replacement for RPMs and other protections. The HSTLD program should not serve as an alternative platform used to scale back rights protection mechanisms (RPMs) and important security policies and procedures or to move them from the Draft Applicant Guidebook to this voluntary certification program. *INTA Internet Committee (8 April 2010).*

Registry –registrar roles.
The snapshot contemplates registries taking responsibility for registrar functions, and for the accuracy and completeness of registrant data. Recent registrar failures have demonstrated the extreme challenges involved in providing such assurances. The snapshot also proposes to alter the fundamental contractual registry/registrar relationship; it thrust registries into a *de facto* enforcement role vis-à-vis registrar functions. ICANN, as the contacting party with registrars, should take whatever action is needed to enforce its contracts with registrars. Further, the snapshot fails to identify the suitable repercussions for registrar noncompliance. *RySG (8 April 2010).*

Regarding Principle 3:

> It is unclear how a registry would be able to guarantee a registrar's internal processes and choices. The reseller level of the distribution chain adds even more complexity and challenges.
>
> Authentication of registrant information at the time of registration may not be reasonable or reliable—socially or technically. E.g., there are no worldwide databases that provide reliable registrant information. Registrars that are located or do business with registrants in certain parts of the world may be at a disadvantage.
>
> Auditing makes the registry operator responsible for the actions of the registrars, and for the results of the program as a whole. Given the other issues raised, what registry operator and independent assessor would take on liability to develop and/or attest to the controls in place?

RySG (8 April 2010).

Proof of concept lacking. It has not been demonstrated if or how the program proposed by the snapshot can deliver better security and reduced malicious activity by the participating TLDs. E.g.:

> Criminals already circumvent registrar-side controls designed to catch fraudulent credit card and contact data.
>
> Regarding authentication, checking to see if an individual or business is in a database does not constitute verification that the entity is purchasing the domain name. Every day criminals register domain names by appropriating the identities and contact data of other people and often obtain that information from databases.
>
> To our knowledge there have not been empirical studies of how domain eligibility policies and procedures affect the amount of e-crime in a TLD (e.g., abuse occurs regularly in some ccTLDs that have nexus requirements).
>
> Registries and registrars cannot control how registrants use the domains, or how registrant servers become infected by malware or hacked for phishing.
>
> A central assumption of the program is that participating registries will be able to bind their registrars to certain requirements and that the registries will be able to choose which registrars they will do business with. This runs contrary to existing equivalent access and nondiscrimination obligations under current ICANN policy that is reflected in current registry contracts.

RySG (8 April 2010).

Improve minimum standards and apply them to all TLDs, new and existing.
The goals being addressed are of such fundamental importance to the secure operation of the Internet that to permit any registry refusing even to consider such changes where such changes advance these aims to continue operating as a registry would not be in the public interest. The HSTLD Review Team should focus on improving the minimum standards for all TLDs, especially existing TLDs such as DotCom, to as far as possible eradicate these problems. To demand improved procedures for new TLDs, which cannot have been affected by the problems motivating this study in the first place, would in effect be an abandonment of those existing TLDs, which hardly does anything for the stability of the Internet. *P. Foody (9 April 2010).*

Approaches to mandatory participation.
The INTA Internet Committee supports greater identity verification for domain names in all TLDs and has advocated some level of mandatory participation in HSTLD to achieve this. An entirely voluntary system will not reach critical mass and will not be able to sustain an independent certification authority. Enhanced identity verification for all gTLDs is needed to avoid further erosion of public confidence in the authenticity of branded goods and services offered on the web. Short of mandatory participation, INTA Internet Committee supports two possible approaches:

> (1) A framework requiring mandatory participation in limited fields, such as fields involving financial subject matter, young audiences, gTLDs that have reached a

threshold of dispute proceeding or proxy registrations, or any gTLD that represents implicitly or explicitly that it has enhanced security (e.g., ".safe"); or (2) A specific preference in awarding gTLDs to applicants that agree to verify identity and prohibit masking.

INTA Internet Committee (8 April 2010).

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 its willingness 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 gTLDs 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? *COA (8 April 2010).*

Malicious conduct—grounds for challenge to gTLD application. Whatever approach ICANN ultimately decides to take regarding 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. *COA (8 April 2010).*

Study lacks a comprehensive approach to the distribution chain. The study appears only to consider the security of the end-destination site and does not appear to address any of the compromises that could occur in the journey from origin machine to destination. E.g., while screening processes for registry employees is understandable, it is unlikely any such employee could cause the sort of problems that a rogue ISP could, yet there does not appear to be any consideration of the role of the ISP in this paper. *P. Foody (9 April 2010).*

Value of HSTLDs linked to security of the whole chain. If we are to rely on the HSTLDs for security, the whole chain must be secured—specifically the process by which HSTLD keys (and other changes) would be incorporated into the root zone. Presently I understand this to be a highly insecure process spread across multiple organizations with little rigor around security processes. The ICANN document "A Model for High Security Zone Verification Program" (11-18-2009) mentions "strong multi factor authentication throughout the name space." ICANN must apply the same to the above part of the chain, otherwise the HSTLD loses its value. There have been many technical proposals to solving this processing insecurity over the years (e.g., changes sent directly to the root maintainer in SMIME signed email by HSTLD operator for validation by the maintainer. This creates a publicly verifiable chain of trust with no opportunity for changes by intermediaries). So I assume the problem is a political one. However, until the same rigorous security practices expected of the HSTLD applicant are put in place, the security of the HSTLD means little. *D. Smiley (10 Mar. 2010).*

Customer service: suggestion for physical contact addresses by registries and other businesses. Could ICANN encourage registries and other businesses such as Yahoo,

Priceline, Expedia, etc. to provide physical contact addresses so that customers writing to those addresses can be provided with written responses on company letterhead, albeit for a small charge, to confirm as far as possible that whatever email correspondence might have been received is genuine and authorized, since email is not the most secure of communications. *P. Foody (9 April 2010).*

Reliable and Accurate Whois Data. The snapshot's proposal to add stronger Whois identity verification for HSTLD registrants is necessary in order to protect the public and brand owners against instances of infringement and malicious conduct. The current lack of policing of Whois data creates such a significant barrier to the enforcement of rights that the INTA Internet Committee considers a thick Whois system an imperative to the HSTLD program. The INTA Internet Committee supports the snapshot's proposal to require that registrants within an HSTLD domain supply detailed and accurate registration information and that registrars and registries agree to police and enforce such requirements. Private registrations in HSTLDs should also be prohibited—this is a prerequisite for HSTLDs being zones in which users can be assured that the site they deal with is what it seems. *INTA Internet Committee (8 April 2010).*

Auditing is essential. Auditing of HSTLD registries, registrars and registrants is essential to earn the trust of Internet users and the reputation necessary for an effective certification mark. Audit processes and enforcement mechanisms for ICANN to certify a registry as a HSTLD will be paramount. ICANN should develop and set forth for comment a proposed audit process and a description of how the HSTLD program will be staffed and funded. *INTA Internet Committee (8 April 2010).*

Marketplace recognition of HSTLD certification. A user-friendly and quick way to identify a domain name with the HSTLD should be designed. If the consuming public is not aware or does not understand the certification mark, then businesses and brand holders will have no incentive to follow the Internet users to a HSTLD (e.g.,. the INTA Internet Committee has discussed the possibility that the HSTLD certification be readily identifiable by Internet users through integration with the user's browser). *INTA Internet Committee (8 April 2010).*

Further identifying the benefits of the HSTLD program. Further work should be done to provide a more robust list of the practical benefits registrants and end users may see from high security zone certification. The HSTLD Advisory Group should consider the manner in which an HSTLD certification program would be marketed to such end users to increase the likelihood of marketplace adoption of high security TLDs. Failure to communicate the benefits will likely mean that the program will generate little interest, particularly if registration of such domains is more expensive than registration in "non-secure" registries. An incentive or business benefit would be to propose that new gTLD applicants that agree to be part of the HSTLD program be awarded more points in the application process. *INTA Internet Committee (8 April 2010).*

ANALYSIS AND PROPOSED POSITION

Comments suggested that the HSTLD program should be mandatory and not voluntary in nature. Related to these comments, other comments also questioned if the HSTLD program was an appropriate role for ICANN to undertake. Although the HSTLD program is still under development (current published documents are concept or development only), currently, the resulting standards created by the HSTLD program will be voluntary in nature. It is important to note that the program is being designed with community input, through the feedback elicited from the High Security TLD Advisory Group (HSTLD AG). The overall position on the voluntary nature of the program may be subject to change, as the ICANN policy development process, through a multi-stakeholder, consensus based process, will ultimately decide the overall course of the HSTLD program. .

Comments questioned the addition of strong incentives to adopt HSTLD program requirements. At this point, the community has not yet discussed incentives for the HSTLD program. These comments will be taken into consideration as a component of HSTLD program development. Again, the creation of incentives may be a policy and not an implementation decision as they could, in effect, create a mandatory program.

Comments supported the concept of a voluntary, high security framework for new gTLD zones, provided the new high security framework is not executed using a "top down" centralized approach. The community is working with ICANN to develop the high security framework, through an advisory group called the High Security Top Level Domain Advisory Group (HSTLD AG). The HSTLD AG represents many stakeholders, and is collaborating on many key elements of the HSTLD program, including the control requirements of the program. Using this development approach, ICANN believes it is developing the HSTLD program through a collaborative, bottom-up approach. See also comments under the HSTLD program origination and execution.

Comments raised specific questions regarding the origination and execution of the HSTLD program, including:

(1) *It is not within ICANN's limited technical coordination mission related to Internet identifiers.* ICANN's current role in the HSTLD program is to function as a coordinator for community development of the program, through the ICANN sponsored HSTLD Advisory Group. ICANN does not believe this is beyond ICANN's mission.

(2) *It would expand ICANN's authority to address malicious uses of domain names.* It is not anticipated that ICANN will offer this program or any certification/verification related to the program directly nor intervene directly in specific incidents where domains are used maliciously, except in consultation with the registry/registries affected. ICANN is currently acting as the overall facilitator for the development of a program that ICANN and the HSTLD AG anticipate will ultimately be offered by a separate administrator, should the program development reach a stage where this is necessary.

(3) *It would put ICANN into direct competition with organizations that already are capable of performing such a function*. ICANN is not seeking to compete with commercial entities in the security field or with registries and registrars. Rather, the HSTLD program has now progressed to the formation of an advisory group that is focused on seeking community consensus on the definition, agreement

and documentation of good and acceptable security controls for use in improving TLD security. The acceptance and application of these controls on individual TLDs is currently anticipated to be a voluntary decision, made by individual TLD operators. In any case, ICANN does not intend to operate the program directly or indirectly. A set of criteria or controls is being developed. Outside agencies can seek to provide the certification service – current "competitors" could provide the service.

(4) *The demand for such zones could be met more effectively by registries in cooperation with existing security organizations.* This is one possible model. The current scope of the HSTLD program includes draft control activities at the registry, registrar and registrant levels. A program run by registries and existing security organizations may have to be augmented with other expertise..

Comments questioned whether the HSTLD program is too focused on TLDs, without focus on other elements of the DNS structure (e.g. ISPs). The HSTLD program concept paper proposed a model. The community is working in collaboration with ICANN on the actual development of the HSTLD program. A possible offshoot of HSTLD program development is that various aspects of the HSTLD program, including the practices and control elements being defined by the program, could serve as a control model for other actors in the name space (e.g. a DNS operator who authoritatively resolved 3rd level labels). The current voluntary based model of the HSTLD program should not be perceived as regulation. Rather, a voluntary based program can represent a method for registries to distinguish themselves in a free market.

Comments requested that the HTSLD program collaborate with existing standards bodies to develop the HSTLD framework. ICANN agrees with this comment that there is no need to re-invent controls that are available from existing standards bodies. Many of the controls currently being evaluated by the HSTLD AG are sourced from the existing standards bodies identified in the comments. Where applicable, the control requirements under consideration by the HSTLD AG provide a reference to the standard that provides the original source of the control. The goal is to allow appropriately qualified external contractors to audit HSTLD controls where existing controls are applicable, and to consider and incorporate controls specific to the domain name system as a complement to standard controls. This goal, the qualities and requirements of external contractors and the mechanism of review are items of focus for the HSTLD AG. ICANN anticipates that for any method of HSTLD program control evaluation selected by the community, appropriate evidence of existence and effectiveness of required HSTLD controls would need to be made available.

Comments opposed a self-certification/report card approach to the measurement of control requirements for the HSTLD program. ICANN will recommend the HSTLD AG take these comments into consideration as they provide recommendations for program development.

Comments suggested that the HSTLD program is not a replacement for rights protection mechanisms (RPMs) or other similar protections. ICANN agrees that the HSTLD program is a discreet issue and is not a replacement for the RPM mechanism.

Comments questioned the role and relationship of registries and registrars in TLDs that elect to adopt the requirements of the HSTLD program. ICANN anticipated that the HSTLD program might create opportunities for market innovation and differentiation around the relationship of the registries and registrars interested in participating in the HSTLD program. Such innovation may include practices in which a registry sets registrar criteria necessary to comply with requirements of the HSTLD program.

Comments suggested that the current HSTLD program concept has not demonstrated if or how the fully developed HSTLD program will deliver better security and will reduce malicious activities by participating TLDs. Once the HSTLD program is fully developed, documented and implemented, practical experience gathered from the TLDs that participate in the program will be available to assess the overall effectiveness of the program.

Comments referenced improved minimum standards for all TLDs, based on HSTLD program requirements. Two possible methods of achieving this goal are:

(1) To impose HSTLD controls through regulation or compliance efforts; or
(2) To impose HSTLD controls for those TLDs that desire the controls, driven by market need.

The current HSTLD model favors market adaptation of the HSTLD program, for TLDs that desire to demonstrate their participation in such a program. As stated earlier – the other model would require policy consideration.

Comments suggested two approaches to mandatory participation in the HSTLD program, including:

(1) Mandatory application of an HSTLD framework for any gTLD that represents implicitly or explicitly that it has or is based on enhanced security. This approach is not currently under consideration by the HSTLD program due to implementation difficulty – impossibility really; and
(2) Mandatory application of an HSTLD framework through specific preference during the gTLD application process. The current gTLD application process, as defined by the current approved Policy does not provide specific preference to new gTLD applicants that wish to adhere to the requirements of the HSTLD program.

Comments requested that ICANN apply the HSTLD program as a potential element of challenge to a new gTLD application. These comments will be taken under consideration under the development of the new gTLD program – although at first blush, such an implementation would require policy work for the reasons stated above..

Comments observed that the current HSTLD program does not seem to take the role of the ISP into consideration. The current HSTLD program focuses on parties with which ICANN has a contractual relationship. ICANN currently does not have contracts with ISPs and would not be able to enforce HTSLD program elements at ISPs.

Comments suggested that the HSTLD program take changes incorporated into the root zone into account during program development. ICANN will work with the HSTLD AG to take this issue into consideration during HSTLD program development

Comments suggested that ICANN encourage registries and other businesses to provide physical contact addresses, so that customers writing to those addresses can be provided with genuine and authorized responses from the registries and other businesses. ICANN will work with the HSTLD AG to take this issue into consideration during HSTLD program development

Comments suggested that the HSTLD program add stronger Whois identity verification. ICANN will work with the HSTLD AG to take this issue into consideration during HSTLD program development.

Comments requested that the HSTLD program propose an audit process and associated enforcement mechanisms for the HSTLD program. ICANN will work with the HSTLD AG to take this issue into consideration during HSTLD program development.

Comments requested that the HSTLD program provide a user-friendly and quick way to identify domain names that participate in the HSTLD program. ICANN will work with the HSTLD AG to take this issue into consideration during HSTLD program development.

Comments requested that the HSTLD program develop a specific list of the practical benefits of the HSTLD program to registrants and end-users. ICANN will work with the HSTLD AG to take this issue into consideration during HSTLD program development.

RESPONDENTS

Coalition for Online Accountability (COA)
Paul Foody (P. Foody)
GoDaddy.com, Inc. (Go Daddy)
International Trade Association Internet Committee (INTA Internet Committee)
Registries Stakeholder Group (RySG)
Dave Smiley (D. Smiley)