DRAFT PROGRAM DEVELOPMENT SNAPSHOT[1]

HIGH SECURITY ZONE TLD

ADVISORY GROUP

[1] Development snapshot taken from HSTLD AG wiki and e-mail list on 2/17/2010

STATUS OF THIS DOCUMENT

This is a development snapshot of the activities completed or in progress of the High Security Zone TLD Advisory Group ("HSTLD AG"). The draft work in this document reflects a continued development effort around a voluntary program designed to support control standards and incentives to increase trust in TLD's that elect to participate in the program.

SUMMARY

We submit this report to the ICANN community for comment as part of the ongoing work in developing the Applicant Guidebook for new gTLDs. Work reflected in this report is considered "work in progress", as we develop a voluntary High Security TLD program.

DOCUMENT STANDARDS

As a development snapshot, content contained within this document is a combination of brief descriptions and actual current state of the program elements currently under development in the HSTLD program. To help make the distinction between program element descriptions, and actual program development content, program element descriptions are in normal text and program development content is in italicized text.

Contents

1.0 EXECUTIVE SUMMARY

Initial work on a voluntary program consisting of control standards and incentives to increase trust in TLD's that elect to participate in the program occurred prior to ICANN's international public meeting in Seoul. During the period of time leading up to the Seoul meeting, ICANN staff created a concept paper outlining initial thoughts on how such a voluntary program might be accomplished. The concept paper was published as a component of the new gTLD Draft Applicant Guidebook version 3 and can be referenced on the following link:

http://www.icann.org/en/topics/new-gtlds/high-security-zone-verification-04oct09-en.pdf

Much of the community response to the concept paper was positive**.** To continue development support of the concept, ICANN has invited community members to participate in an HSTLD Advisory Group ("HSTLD AG"). The HSTLD AG currently consists of members of ICANN staff and members of the community that have expressed an interest in assisting with the program as well as individuals who are subject matter experts in disciplines related to the program (e.g., security, auditing, certification programs). The HSTLD AG meets regularly to build upon the concepts introduced in the original paper, draft control elements and program requirements, and publish an actionable program for community consideration and review. This paper presents the most recent materials under review or development by the HSTLD AG.

The HSTLD AG conducts its activities and program development through an open and transparent process. This development snapshot is a component of this process. Additional information including group participants and recordings of the HSTLD AG weekly meetings are available at the following link:

http://www.icann.org/en/topics/new-gtlds/hstld-program-en.htm

2.0 DEVELOPMENT ACTIVITIES

The most significant development activities to occur since ICANN's international public meeting in Seoul Korea include:

- Formation of the HSTLD AG and HSTLD AG review of the original concept paper;
- Documentation of original HSTLD requirements and rational;
- Additional work to improve original concept paper content including foundational components:
  - Group Goal Statement
  - HSTLD Problem Statement
  - HSTLD Benefits Statement;
- Additional work to improve original concept paper Principles, Topics, Objectives, Sample Criteria; and
- Addition of a new "report card" concept.

The remainder of this development snapshot document will explain each of the activities above, and present their current state of development as a "snapshot" in time. The HSTLD AG uses its weekly meetings, e-mail, an HSTLD AG wiki and other collaboration tools to develop the HSTLD program material. Ultimately, the material created by the HSTLD AG will be used to create the key elements of and actionable HSTLD program. The AG will then publish the program available for public comment.

2.1 Formation of the HSTLD AG

Work began on the improvement of the voluntary HSTLD program concept through ICANN's sponsorship of an advisory group that is composed of ICANN staff and interested members of the community. The group was formed to continue to develop the voluntary HSTLD concept material originally published as a component of ICANN's international public meeting in Seoul Korea. The first meeting of the HSTLD AG occurred on January 6th 2010 and the group continues to meet on a once per week schedule, to work on the development of the HSTLD program concept. Status of the group's development efforts, development snapshot updates and ultimately a new concept paper (should the program be considered release) will be reported during ICANN's international meetings.

2.2 Documentation of Original HSTLD Requirements and Rational

As the HSTLD AG was forming, the group enumerated the original requirements and rationale for the HSTLD concept paper, to help with the development of core material. This material was gathered and can be referenced on the following link:

http://mm.icann.org/pipermail/hstld-ag/2010-January/000094.html

2.3 Overview of Development Material

One of the first areas of focus for the HSTLD AG was the HSTLD Group goal, problem and benefit. These areas form the foundation of a well executed HSTLD program, and serve as the overall guidelines that the HSTLD program is based on. HSTLD AG discussion has progressed beyond these areas for the moment, but they will be revisited as necessary through the overall HSTLD development effort.

During the development of the goal, problem and benefit statements, members of the HSTLD AG suggested a new method of reporting, for the TLD's that are interested in becoming an HSTLD TLD. The new method of reporting is based on a "report card" concept. It provides a method for TLD's to self-certify their compliance with HSTLD program. The AG will evaluate this reporting method and compare against other certification, trust mark, and similar verification programs.

After the HSTLD goal, problem and benefit material was created and discussed, the HSTLD AG focused on the principles, topics, objectives and sample Criteria. This material is the most recently discussed material and is still being actively developed.

Each of these sections will be described briefly below, with a normal text forward describing the material, and the HSTLD AG working draft material in italics.

2.4 Group Goal Statement

The first development task undertaken by the HSTLD AG was to craft an HSTLD AG group goal statement. The HSTLD AG group goal statement provides the community a charter of the overall goal of the HSTLD AG. It provides a method of communicating the overall goal and direction to the community and to HSTLD AG members. The current draft HSTLD AG goal statement is as follows:

"The goal of the High Security Zone Top Level Domain Advisory Group is to bring together community representatives to evaluate the viability of a voluntary program, supporting control standards and incentives that could potentially be adopted to provide an enhanced level of trust and security over the baseline registration-authority controls."

2.5 Group Problem Statement

As the HSTLD AG began to craft an appropriate goal statement, several AG members raised the issue of defining what problems the HSTLD AG was formed to solve, so that these problems were documented and available for community review. This material will help to maintain HSTLS AG focus, as controls designed to reduce these problems are produced. The HSTLD AG problem statement is as follows:

"Certain individuals/organizations have sought to exploit vulnerabilities within the DNS technology, and the business practices of certain registration authorities, for inappropriate and/or illegal purposes. The exploitation of these vulnerabilities has threatened the security and stability of the Internet, and negatively impacted the trust users have when using the Internet.

There are several interested parties:

1 *Registrants would like to be sure that the name they register doesn't get hijacked through registrar/registry/their-own account compromise. (Including DNS, WHOIS, etc)*

2 *Registrars would like to be able to give reasonable guarantees to Registrants that #1 won't happen because they have controls. In order to do so, they require both Registrant and Registry cooperation.*

3 *Registries would also like #1, and this requires the cooperation of Registrant and Registrar.*

4 *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.*

5 *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."*

2.6 Group Benefits Statement

The final foundational area of program development to date is the development of an HSTLD AG benefit statement. The ultimate purpose of the benefit material is to help the community understand what benefits could be achieved through the adherence to an HSTLD program. This material is not meant to be a comprehensive business benefit analysis. Rather, it is meant to provide overall community benefits, broken down by the groups most impacted by the HSTLD program. This current HSTLD AG benefit material is as follows:

"Registries benefit:

Ry1. by demonstrating that they have a high standard for continuity, security and operational integrity through a auditing process

Ry2. by demonstrating that they have business operations which been reviewed and have met standards for organizational, operational and financial integrity

Ry3. by demonstrating that they have data processing, storage, and methods which satisfy high standards for data confidentiality, accuracy, integrity, recovery, etc.

Ry4. by demonstrating that they have implemented practices and measures to mitigate abuses of domain name service and domain registration services

Ry5. by satisfying (Ry1) thru (Ry4), which instills trust in end users and registrants that their businesses are financially sound and trustworthy, and assures that their measures to reduce the incidence of malicious domains registered are enforced by registrars who process registrations for the registry

Registrars benefit:

Rr1. by demonstrating that they have satisfied all standards for continuity, security and operational integrity that "trickle down" from a HSTLD registry through an auditing process. ("trickle down" means that the registrar enforces any condition that is imposed on the registry that cannot be met without the assistance of the registrar, e.g., a condition that affects the registrar-registrant interface)

Rr2. by demonstrating that their business operations have been reviewed and met standards for organizational, operational and financial integrity that "trickle down" from a HSTLD registry

Rr3. through "trickle down" of Ry3

Rr4. through "trickle down" of Ry4

Rr5. by satisfying (Rr1) thru (Rr4), which instills trust in users and registrants that the HSTLD trusts the registrar to process registrations on behalf of the registry. The higher standards for *registration processing also assure users and registrants that registration data are accurate, that abuse complaints are processed according to standard practices, etc.*

Registrants benefit:

Re1. by demonstrating that they are willing to submit to a stringent verification measures associated with a HSTLD registry

Re2. by demonstrating that they are willing to maintain accurate registration data (and comply with verification measures implemented to ensure the data are accurate)

Re3. by demonstrating that they are willing to agrees to terms of service and AUP that enumerate prohibited uses and abuses and empower registry/registrar with suspension or other responses when dealing with TOS/AUP breaches

Re4. from measures implemented to mitigate malicious domain registrations: many of the same measures make it more difficult for attackers to compromise a legitimate registrant's account

Re5. from measures implemented to mitigate abuse of DNS: many of the same measures make it more difficult for attackers to compromise a legitimate registrant's account and then alter DNS configuration info.

Users benefit:

U1. from more accurate registration data

U2. from lower incidents of malicious registrations and DNS abuse among domain names registered in a HSTLD

U3. from clearly defined abuse handling processes"

2.7 "Report Card" Concept

As the HSTLD AG developed the foundational material above, questions were raised regarding the original verification concept paper's certification process. The original concept paper used a method of 3rd party certification as a mechanism to report TLD adoption of the HSTLD program controls to the overall community. Through the process of group discussion, an alternate (although not mutually exclusive) method of TLD adoption of HSTLD controls was introduced. The alternate method is based on the concept of a report card that TLD's can fill out to report their level of HSTLD control compliance to the community. A very general overview of the concept is as follows:

"TLD Security Scorecard

Currently ICANN provides no metrics to empower registrants to make an informed decision about their domain name registration options. The Security Scorecard would be a concept that could be integrated into ICANN's current dashboard features.

This scorecard would comprise a matrix of agreed upon security control criteria on the Y axis, and "all" TLD registry operators on the X axis. Each box in the matrix would comply with the following color scheme:

- *White/Blank Box: The registry operator has provided no data in connection with that control element.*

- *Yellow Shaded Box: The registry operator has "self certified" their compliance with that control element.*
- *50% Green Shaded Box: A third party has verified the registry's compliance with that control element at a specific point in time, but has not been able to establish a long term compliance.*
- *100% Green Shaded Box: A third party has verified he registry's compliance with that control element over a long term compliance period.*
- *Red Shaded Box: In a circumstance where a registry "self certified" a specific control criteria but was then found to be in noncompliance. It is envisioned that any false statements regarding self certification would be a violation of the registry agreement and would be investigated by ICANN compliance staff."*

2.8 Principles, Topics, Objectives, Sample Criteria

Section 3.2.1 of the original concept paper contained details about the HSTLD program's core requirements. This section represents a collection of principles, objectives, and criteria that form the basis of the actual controls that are designed to improve TLD security and trust. The HSTLD AG has been working to improve this section. Most recently, the original principles were reviewed and an additional draft principle (currently listed as "Principle 4") is being discussed for eventual addition to the principles. The HSTLD AG is also currently evaluating the "possible criteria topics", in an effort to agree on actual criteria and supporting illustrative control examples. When fully completed, each criteria topic will have one or more illustrative control examples that provide guidance for an appropriate control necessary to meet the criteria requirements. The current development snapshot of this section is as follows:

"PRINCIPLE 1: The Registry maintains effective controls to provide reasonable assurance that the security, availability, and confidentiality of systems and information assets supporting critical registry IT (i.e., registration services, registry databases, zone administration, and provision of domain name resolution services) and business operations are maintained by performing the following:

- *defining and communicating performance objectives, policies, and standards for system and information asset security, availability, confidentiality, and privacy;*
- *utilizing procedures, people, software, data, and infrastructure to achieve defined objectives in accordance with established policies and standards; and*
- *monitoring the system and information assets and taking action to achieve compliance with defined objectives, policies, and standards.*

No.	*Topic*	*Objective*	*Possible Criteria Topics*	*Criteria*	*Illustrative Controls*
1.1	*Registry IT Infrastructure Security*	*Key elements of the IT components that support the TLD infrastructure are secured and appropriately protected from unauthorized physical and logical access.*	*· Security management* *· Personnel security* *· Physical access control* *· Media storage and disposal* *· System acquisition and development controls* *· Security incident management controls* *· Security incident response and*		

			reporting *· Interface controls* *· System access management* *· Network security* *· Application security* *· Encryption requirements* *· Periodic vulnerability testing and response exercises* *· System software release process* *· Name resolution service management controls (e.g., DNS zone integrity and name server availability monitoring, …)* *· DNSSEC deployment plan* *· Secure communications channels (authenticated, encrypted connections with registrars)* *· Information asset management (database accuracy/integrity/availability services for zone, registration and other customer data)*		
1.2	*Registry IT Infrastructure Availability*	*TLD services are available for use per contract or commitment.*	*· Service level agreements* *· Whois service availability* *· Whois service performance level* *· Whois service response times* *· Whois accuracy and completeness* *· Availability monitoring* *· Registration and transaction data escrow including escrow schedule, specifications, transfer, and Security Verification* *· Disaster recovery and business continuity plan (failover practices, including plans to sustain name resolution service in the event of a business failure) and exercises* *· Environmental controls (power and air conditioning, fire protection, generators)* *· Cabling security controls*		
1.3	*Confidentiality and Privacy of Sensitive Data*	*Information owned, managed or transferred through the TLD that has been designated as confidential is protected as*	*· Appropriate classification of confidential and personally identifiable information* *· Data collection, use, retention, access, and disclosure policies*		

		committed or agreed. Personal information collected by the TLD operator is collected, used, retained, disclosed, and destroyed appropriately, in line with relevant data protection laws per the jurisdiction of the registry operator.	*· Data at rest and in transit* *· Third party access to information* *· Encryption requirements* *· Management controls for signing keys* *· Physical and logical access controls* *· Segregation of duties* *· System monitoring* *· Personal security controls*		

PRINCIPLE 2: The Registry maintains effective controls to provide reasonable assurance that the processing of core Registry functions are authorized, accurate, complete, and performed in a timely manner in accordance with established policies and standards. The identity of participating entities is established and authenticated.

No.	*Topic*	*Objective*	*Possible Criteria Topics*	*Criteria*	*Illustrative Controls*
2.1	*Registry Security Verification*	*Registry operator credentials are made available to substantiate the identity of the legal entity that operates the TLD.*	*· Vetting of REGISTRY organization, including* *- Background of principals* *- Verifiable address* *- Verifiable e-mail address* *- Verifiable telephone numbers* *- Articles of incorporation* *- Certificate of formation* *- Charter documents* *- Business license* *- Doing Business As (i.e., assumed name)* *- Registration of trade name* *- Partnership papers* *- Business license* *· Insurance coverage* *· Financial capabilities* *· Revalidation requirements* *· Screening processes for employees*		
2.2	*Registrar Security Verification*	*The identity of the Registrar is designated and established prior to commencement of operations*	*· Vetting of REGISTRAR organization topics noted in 2.1* *· Registrar accreditation status* *· Revalidation requirements*		
2.3	*Registry Processing Integrity*	*TLD data is consistent and correct at the TLD Registry level.*	*· Domain name registration and maintenance* *· Maintenance, accuracy, completeness, and integrity of public*		

			Whois data · Vetting of new registrar · Ongoing monitoring processes · Registrar data QA/quality review (and escrow data audit results) · Dispute resolution process		
2.4	Anti-abuse Policy and Enforcement	Establish effective controls to reduce malicious conduct by Registrars and Registrants	· Anti-phishing and anti-spoofing controls for new TLDs · Independent third party rating(s) from reputable anti-phishing and anti-malware analysts and laboratories · SLA based on percent of malicious domains per ”unit measure” of registrations (e.g., 1000, 5000, 10,000 domains) · Orphaned name server policy (statement of what actions will be taken to identify and correct orphaned name servers) · Abuse points of contact with a documented response process that is timely and auditable · Definition of malicious use (conduct), explicit prohibition of malicious conduct in registrant terms of service agreement · Rapid Domain Suspension process · Thick Whois process and support · DNSSEC & IPv6 deployment plan · Real-time zone monitoring (e.g., for suspicious activity, e.g., fast flux) · Monthly reports of malicious activity reported to registry (such as phishing and botnets) and commitment to address if results are high (relative to other registrars who do business with this registry)		

PRINCIPLE 3: The Registry shall maintain effective controls to provide reasonable assurance that the processing of core Registrar functions by its Registrars are authorized, accurate, complete, and performed in a timely manner in accordance with established policies and standards. The identity of participating entities is established and authenticated.

No.	Topic	Objective	Possible Criteria Topics	Criteria	Illustrative Controls

3.1	Registrant Security Verification	Registrant identity is verified and established prior to provisioning of domain name by the Registrar.	· Vetting of organization topics noted in 2.1 · Authority of Registrant to register in the TLD · Commercial users exempt from Proxies/Anonymous Registrations (applicant must provide proof that the applicant is a natural person, organization must show cause or justification for anonymity)		
3.2	Registrar Processing Integrity	Data is consistent and correct at the Registrar level.	· Registrar authenticating new registrants through agreed processes · Registrar confirmation that registration data are accurate and complete · Registrar monitoring registration data for accuracy and completeness · Registrar authentication of registration data for each transaction · Registrar confirmation of change in registration data · Rejection/suspension of registration data with cause (incomplete, false/inaccurate) · Thick Whois · Registrar removal of registration data · Ongoing monitoring processes · Periodic QA review of registrant data · Takedown process and timeliness objectives (e.g., MTTR)		

PRINCIPLE 4: Registrants in a High Security Zone are expected to maintain current and accurate information, and to commit to refrain from activities designed to confuse or mislead the Internet-using public.

No.	Topic	Objective	Possible Criteria Topics	Criteria	Illustrative Controls
4.1	Registrant Data Accuracy	Registrants provide current and accurate identity and locative information	WHOIS data Registrant locative information provided to registry Contact information provided to registry Absence of proxies		
4.2	Registrant Conduct	Registrants will explicitly commit to abiding by ICANN's policies, as well as any additional obligations created through the application of HSTLD standards	Code of Conduct”		

3.0 NEXT STEPS

The HSTLD AG will continue to develop material in an effort to improve the original HSTLD concept paper. Immediate next steps include but are not limited to continuation of the group's weekly meetings, meeting in Nairobi, and continued development of key program material including:

- Foundation material;
- The "report card" concept vs. alternative options;
- Principles, objectives, criteria and illustrative examples; and
- Overall program governance and actors.

As mentioned previously, development snapshots and updates to the original concept paper will be published during ICANN's international meetings.