Internet Corporation for Assigned Names and Numbers
Request for Information
High Security Zone Verification Program

Please fill-in the form and submit it to hstldrfi@icann.org not later than 21 October 2010.

Full Company Name:

Type of Company:

Parent Company Name:

User Salutation: ☐ Mr. ☐ Ms. ☐ Mrs. ☐ Dr.

First Name:

Last Name:

Job Title:

Mobile: (please include country & city code)

Fax: (please include country & city code)

Official e-mail address:

Office Address:

City:

Postal Code:

Country:

Address of Internet website:

Alternate contact person: (name and contact details)	

Please review the preliminary background information and answer the questions specified below:

1 Introduction

1.1 Subject

The Internet Corporation for Assigned Names and Numbers (ICANN), in cooperation with its community, has developed a proposed voluntary program consisting of control elements to increase security and trust in the Domain Name System (DNS) for those Top-Level Domain (TLD) registry operators that elect to participate in the program.[1] The concept paper for the program, Model for a High Security Zone Verification Program (the "HSTLD Program"), can be found at http://www.icann.org/en/topics/new-gtlds/high-security-zone-verification-04oct09-en.pdf.

This purpose of this Request for Information (RFI) is to assist ICANN in collecting additional information from prospective contractors and other interested parties that would enable the High Security TLD Advisory Group to assess and shape the viability of the HSTLD Program in completing its work on this project.

1.2 Background

In today's Internet-enabled society, domain names are critical assets for individuals and organizations. Certain individuals or organizations have sought to exploit vulnerabilities within the DNS for malicious or criminal purposes. These individuals and organizations exploit vulnerabilities in processes associated with domain name registration services or DNS administration. The attacks are numerous and varied and include (a) registration of domain names for fraudulent purposes, (b) theft or "hijacking" a domain name away from the rightful registrant, and (c) alteration of DNS information to facilitate phishing, malware downloading, and other "redirecting" attacks. Such attacks threaten the security and stability of the Internet, and negatively impact the trust users have when using it.

ICANN and its community are committed to mitigating the extent to which domain names or the DNS are exploited for malicious purposes. ICANN, with its community, has developed a working framework of principles, criteria, and control standards that would allow TLD registry operators interested in achieving designation as a High Security Top-Level Domain to effectively employ enhanced security-minded practices and policies. The current working framework of principles and criteria form the basis for the core requirements of the HSTLD Program, and can be referenced in the HSTLD Snapshot #2[2]. The HSTLD Program offers a TLD registry an opportunity to voluntarily submit to a third party assessment, resulting in verification that its business and technical operation meet a set of defined criteria (control elements).

---

[1] This includes both generic top-level domains (gTLDs) such as .COM, .ORG, .COOP and .ASIA as well as country code top-level domains (ccTLDs) such as .UK, .DE and .CN.

[2] The HSTLD Snapshot #2 can be found at http://www.icann.org/en/topics/new-gtlds/hstld-program-snapshot-2-16jun10-en.pdf.

As such, the HSTLD Program will be available to any TLD registry operator that finds such verification desirable. By satisfying the criteria for the HSTLD Program, the registry would be distinguished as a High Security TLD through a certificate, trust mark, scorecard or other means. The HSTLD Advisory Group is particularly interested in hearing from Respondents on their experience about the potential pros and cons associated with each of these models, e.g., certificate, trust mark, scorecard.

It is currently envisioned that this HSTLD Program would involve one or more independent third party evaluators. ICANN would maintain a list of approved evaluators and retain oversight and authorship of the control elements. However, the HSTLD Advisory Group is open to hearing from organizations with experience on other possible implementation models/constructs.

The HSTLD Program is intended to mitigate certain malicious and criminal activities that are inside the sphere of influence of the TLD registry operator. For example, the HSTLD Program cannot prevent the use of obfuscated URLS in phishing emails. Additional measures will still be needed to combat these and other tactics commonly employed by some attackers.

2 Considerations and Assumptions

Respondents are expected to be familiar with domain name registration system and DNS ("name service") operations. A short summary is provided below to highlight particular aspects of these systems that are relevant to this RFI.

Domain names are assigned in a hierarchical manner from an originating root level ("."). The labels (delegations) assigned directly below the root level of the domain name system are called Top-Level Domains. There are a number of diverse business models within the domain name space, a sampling of which are detailed below.

TLD registry operators also provide Domain Name Service ("DNS") for the domain names delegated within their Top-Level Domain. In some cases, a TLD registry's DNS infrastructure has a global footprint, i.e., it is geographically dispersed, highly redundant, and able to support billions of DNS transactions daily. Other TLD registries may only contain several thousands of domain names and the DNS infrastructure will be sized accordingly.

Domain name registration services exist to allow individuals or organizations to choose and register a label assigned within a TLD. These second-level labels are connected with the TLD to form a domain name (also called domain, for short) such as example.com, icann.org, or internic.net. Many domain name registration business models exist: for example,

- An ICANN generic TLD registry operator is contractually obliged to provide all ICANN accredited registrars with equal access to the ability to process domain name registrations for labels assigned from its TLD. This results in a fan-out from registry operator to registrar on the order of 100s of accredited registrars.
- ICANN accredited registrars may operate retail or wholesale businesses. Wholesale-model registrars may have 100s or 1000s of resellers and this further fans out the registration service.
- A ccTLD registry operates independently from ICANN and may offer registration services directly to individuals or organizations.

- A ccTLD registry may also engage contractors to perform registration services on its behalf. These contractors may be ICANN accredited registrars (which may be wholesale or retail business operators) or other independent parties.

Like registries, registrars vary in size. Some registrars sponsor hundreds of domains and have dozens of customers, whereas others may sponsor millions of domains registered for millions of customers.

Given this description and "landscape", Respondents are asked to discuss how both point-in-time and periodic assessments of a TLD registry operator based on the HSTLD Program requirements and assessment methods described in the previously referenced concept paper could be conducted.

Respondents are asked to propose a potential implementation process to determine that the registry satisfies the business and operational criteria for High Security Zone designation. The assessment must also include means for verifying registrar operations. Section 3.1.1 of Model for a HSTLD Program identifies the program elements, objectives and sample criteria for these assessments. For example, the evaluation process might include documentation review, interviews, and either on site or remote assessment analysis or monitoring.

Respondents are also asked to consider the following assumptions in formulating responses to the questions listed below.

Scope. The HSTLD Program is available to any operator of registries of delegated branches of the gTLD domain name space such as .BIZ, .COM, .INFO, .NET, .ORG or to any ccTLD registry operator that may find such verification desirable or necessary. Individual registries that volunteer to participate would directly contract program assessors and assessments would be performed at the registry's location(s). The assessment would determine how the registry's services (and those of the registrars who seek to meet the security criteria imposed by the registry) meet (or fail to meet) the enumerated control elements. Assessment time could vary based on the size or complexity of the registry operator. Respondents are invited to comment on the issues related to implementing a program of this scale in questions below.

Criteria. It is assumed that the HSTLD Program elements would provide the basis for enhanced security and trust for the registries that elect to participate. Respondents are invited to comment on the completeness and suitability of the HSTLD Program elements identified in Model for a High Security Zone Verification Program, Section 3, *Elements of a High Security Zone Verification Program* in the questions below. In addition, Respondents are encouraged to identify any industry "best practices" that may not be expressly mentioned in the HSTLD Program requirements. These features may be added to the baseline criteria or may be considered "value added" features that are beyond the baseline expectations.

Goal. The objective of the HSTLD Program is to allow TLD registry operators to voluntarily demonstrate enhanced security operations by establishing and successfully executing control activities necessary to comply with the standard HSTLD Specific Criteria Objectives, as determined by a qualified third party assessor. Potential HSTLD Program assessors are invited to comment on whether the HSTLD Program will meet this objective.

Public Proof of Verification. Respondents are invited to comment on how to represent the verification status of the participating registry. In particular, we seek Respondents' perspectives on the suitability or efficacy of checklists, seals, trust marks or other scoring systems for publicly displaying verifications of this kind.

3 Questions

1. **What is your particular experience with ICANN, or any other organizations/parties (e.g., registries, registrars) that interact with ICANN?**

2. **What is your experience with security mechanisms, controls, auditing, or similar activities?**

3. **How would you propose both point-in-time and periodic assessments of a TLD registry operator based on the HSTLD Program requirements and assessment methods described in the referenced concept paper?**

4. **Describe a potential implementation process to determine, through documentation review, interview, on site or remote assessment analysis or monitoring, or other means that a registry satisfies the business and operational criteria of a High Security Zone TLD.**

5. **How would your assessment consider supporting registrar or reseller operations? Section 3.1.1 of Model for a High Security Zone Verification Program (the "HSTLD Model") and the HSTLD Control Work Sheet (see Appendix A of the HSTLD Snapshot #2) identifies the HSTLD Program elements, objectives and sample criteria which would be used for these assessments.**

6. **What are the considerations in expanding verification beyond just registry operations to include registrar, reseller and potential registrant operations from both an implementation and cost perspective? See e.g., the HSTLD Model, Section 3.1.1 principles 1.3, 2.2, 2.4, 3.1, and 3.2; and the corresponding HSTLD Control Worksheet Criteria Controls, including illustrative control examples.**

7. **In order to determine the potential viability of the HSTLD Program within the domain name marketplace it is critical that prospective participants have an idea of the potential cost of this verification program.**

    a. **Respondent should provide a range of costs seen in connection with other verification programs they have been involved in.**

b. **Based on these other programs, Respondent should provide a range of costs that registry operators might incur in connection with the different models identified in Section 2.**

c. **Based on these other programs, Respondent should provide a range of costs that registrar might incur in connection with the different models identified in Section 2.**

d. **Based on these other programs, Respondent should provide a range of costs that registrants might incur in connection with the different models identified in Section 2.**

8. **Are there any HSTLD Control Worksheet Criteria Objectives or Controls that should be removed or amended? If so which ones, and why?**

9. **Are there any HSTLD Control Worksheet Criteria Objectives or Controls that have not been included, but should be, and if so which ones and why?**

10. **What would you envision to be a reasonable timeframe for developing and implementing the HSTLD Program?**

11. **The HSTLD Advisory Group is particularly interested in hearing from Respondents on their experience about the potential pros and cons associated with various ways of publicly representing an entities verification status, e.g., certificate, trust mark, scorecard.**

12. **Please discuss your perspective on the opportunities and challenges associated with establishing an HSTLD Program and how such a program could be built for success. Describe the elements you believe are critical to creating an effective program, and suggest strategies to address any problems or issues you see with the work that's been done to date.**

4 Important Notice and Disclaimer

This Non-Binding Request for Information and any of its parts, as well as any information, advice or data subsequently provided to the Respondent whether orally or in writing by or on behalf of ICANN, shall be subject to the terms and conditions set out in this RFI or any other specific agreement entered into by the Respondent and ICANN. Therefore, upon having access and receiving any or all of the information contained herein by any means of communication, the Respondent agrees to comply with all the terms and conditions contained herein.

This RFI does not constitute an offer nor is it an invitation or solicitation for any Respondent or any other person to become a provider of products or services to ICANN or any member of the Internet community. Each Respondent must make its own independent assessment and investigation of the information contained herein, and should not rely on any statement or on the significance, adequacy or accuracy of any information contained in this RFI.

The information contained or referenced herein does not purport to contain all of the data that a Respondent may deem necessary to provide its response. The information contained or referenced herein may not be deemed adequate or appropriate for all prospective Respondents, and it is not possible for ICANN to know the objectives, financial situation and particular needs of each Respondent having access to the information contained herein. Some Respondents may have a better knowledge of, or access through their own business activities to, more information concerning the information requested by this RFI than other Respondents. In all cases, before acting in reliance on any of the information contained or referenced herein, the Respondent should conduct its own investigation and analysis in relation to this RFI, as well as to its accuracy, completeness and reliability; in case of doubt, the Respondent should strive to obtain independent and specific assistance from appropriate professional advisers.

In this regard, ICANN makes no representation or warranty as to the accuracy, completeness, reliability and timeliness of any information contained or referenced in this RFI. ICANN and any of its agents, employees and consultants shall incur no liability for any statements, opinions, information or matters, expressed or implied, arising out of, contained in or derived from, or any omissions from, the information contained or referenced in this RFI. ICANN will not be responsible for, nor will it pay for, any costs, expenses or losses which may be incurred by a Respondent or its representatives in conducting their review and evaluation of this RFI, in expressing interest or submitting an RFI Response, or in any other way arising from, or connected with, this RFI. The information contained and referenced in this RFI is of a preliminary nature and, in light of the above, subject to clarification and change. ICANN may, at its absolute discretion, update, amend or supplement the information contained or referenced in this RFI.

ICANN may also, at its absolute discretion, amend or discontinue this RFI or any procurement processes contemplated herein at any time and without any further notice. All costs related to responses to this RFI shall be borne by the Respondents. All references to currency shall be in US Dollars unless expressly stated otherwise. References to years concern calendar years starting on 1 January and ending on 31 December, unless otherwise stated. No representation or agreement made by or on behalf of ICANN in relation to this RFI or its contents shall be binding on ICANN unless that representation or agreement is made in writing and incorporated into contractual documents to be formed on the basis of this RFI or any subsequent procurement processes issued by ICANN, as the case may be.