

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: **BITS/The Financial Services Roundtable**

Type of Company: **Trade Association**

Parent Company Name: **The Financial Services Roundtable**

User Salutation: **Mr.**

First Name: **Leigh**

Last Name: **Williams**

Job Title: **BITS President**

Mobile: **202-207-8744** (please include country & city code)

Fax: **202-628-2492** (please include country & city code)

Official e-mail address: **Leigh@fsround.org**

Office Address: **1001 Pennsylvania Avenue, NW, Suite 500 South**

City: **Washington, DC**

Postal Code: **20004**

Country: **USA**

Address of Internet website: www.bits.org; www.fsround.org

Alternate contact person: **Greg Rattray, Greg@fsround.org, 202-589-2442**
(name and contact details)

BITS

FINANCIAL SERVICES
R O U N D T A B L E

October 18, 2010

Mr. Rod Beckstrom
CEO and President
Internet Corporation for Assigned Names and Numbers
4676 Admiralty Way, Suite 330
Marina del Ray, California 90292

Re: Response to ICANN RFI on HSTLD Verification Program

Dear Rod:

BITS, the technology policy division of The Financial Services Roundtable, appreciates the opportunity to comment on ICANN's program to establish a HSTLD program. BITS continues to support the efforts of ICANN and its community to mitigate the extent to which domain names or the DNS are exploited for malicious purposes and further believes that effective programs must be in place to ensure control over malicious conduct before proceeding with the launch of new gTLDs, especially those principally focused on providing banking and finance services.

BITS supports and has been actively engaged in the community advisory group effort to establish a HSTLD verification program as an essential element of ICANN's responsibility to mitigate malicious conduct. We are committed to the success of the HSTLD program and plan to continue our support for the community advisory group, ICANN staff and when selected, the eventual implementing organization for the program in terms of control requirements, processes for verification and approaches to establishing seals or trust marks.

BITS assumes the HSTLD verification program certifying that the operations of a TLD meets a set of defined control elements will be

in place before ICANN accepts applications for new gTLDs principally focused on providing banking and finance services. Further, BITS believes that compliance with this program must be mandatory for such applicants. BITS has consistently engaged ICANN regarding the need for strong controls related to TLDs providing banking and financial services through comment on all versions of the Draft Applicant Guidebook, specific input on controls necessary for new gTLDs providing such services and actively participation in the HSTLD Verification Program working group. The requirement for mandatory controls for operations in new gTLDs principally focused on providing banking and finance services has been highlighted consistently by BITS and other banking and financial services organizations.

BITS is gravely concerned about the recent comment of the ICANN Board regarding this program. The RFI states “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 25 September 2010 resolution of the Board states, “the development of the concept does not impact the launch of the gTLD application process.” The Resolution goes further in stating that “ICANN will not be certifying or enforcing the HSTLD concept” and “ICANN will not endorse or govern the program.” BITS believes this contradicts the original intent for ICANN to establish this program. Additionally, we believe the lack of ICANN sponsorship for the program will likely undermine incentives for a third-party to undertake establishing such a program. Without such a program, BITS will strongly object to establishment of new gTLDs principally focused on providing banking and finance services.

Our answers to the specific questions posed in the RFI are attached.

Please contact the undersigned (leigh@fsround.org), or BITS Senior Vice President for Security Greg Rattray (greg@fsround.org), if you require any additional information.

Best regards,

A handwritten signature in black ink, appearing to read "Leigh Williams". The signature is fluid and cursive, with a long, sweeping tail on the final letter.

Leigh Williams
President

BITS Responses to High Security TLD RFI Questions

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

BITS has been an active participant in the ICANN multi-stakeholder processes since 2007. BITS is a member of the ICANN business constituency group. It has been actively engaged in commenting on the new gTLD program and provided input on all four versions of the Draft Applicant Guidebook. BITS member organizations are major users of DNS services with a focus on ensuring those services can be used securely. As an organization, BITS has actively engaged with registries related to discussing how a high security zone for financial activities can be established.

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

BITS is a leader in working with its members to improve the security of the banking and finance sector. BITS has an established security program focused on the development of best practices and appropriate controls for this industry since 1996. The comments of BITS regarding the need and criteria for a HSTLD program have been a driver for this effort.

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?

BITS believes both aspects of assessment are necessary and that the methods used need to be consistent with existing industry practices used to validate compliance with other security standards such as ISO 27001. To the extent possible, the program should leverage the efforts of participants in documenting controls and achieving compliance with other regulatory or voluntary programs to the extent possible.

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.

While BITS does not currently plan to be the implementing organization of such a program, we believe it should be consistent with our comment on question 3 above.

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.

BITS believes it is essential to have the scope of controls required to be certified as a HSTLD to include those involving registrars as well as ensure these controls are extended to resellers to include registry and registrant security verification, anti-abuse policy and enforcement and registrar processing integrity.

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.

BITS believes evaluation of potential implementing organizations must include their willingness and ability to extend the evaluation of controls to registrar, reseller and potential registrant operations for a registry seeking HSTLD certification.

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.

As BITS does not currently plan to become an implementing organization for this program, we have not endeavored to answer this question in detail. In general, BITS believes potential costs can be mitigated by an implementation approach that leverages existing control programs that organizations at all levels should have in place as parties participating in the operation of a HSTLD.

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

BITS believes the HSTLD Control Objectives and Controls developed by the working group provide a strong foundation for the establishment of a program. We believe the implementation of the program must include processes to revise and add to controls gleaned from experience as well as to ensure a high level of trust and security can be maintained in the face of evolving threats.

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?

See answer to question 8.

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

BITS believes that the existence of this program is a precondition to the possible establishment of gTLDs that are principally focused on providing banking and financial services. As stated in our cover letter, we believe certification under such a program should be mandatory. BITS believes the HSTLD verification program must be in place before applications for new TLDs principally focused on providing banking and financial services are accepted. BITS believes that no application for a financial generic TLD should be approved unless it includes a commitment to a high security verification program. More generally, BITS is interested in raising the level of security across the existing TLD system. BITS members are contending with the security limitations of operation in many existing TLDs and we strongly support a rapid development and implementation of the program even beyond concerns related to the launch of new gTLDs.

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.

BITS' experience with a variety of trust marks suggests that well-defined certification programs, incorporating clear requirements and public attestations, can be highly successful at standardizing and

communicating elevated levels of control. Seal programs are most valuable to consumers and business partners when they are highly uniform, as in mandatory programs, and when their scope is well-defined, as in the gTLD environment.

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.

BITS commends the efforts of the ICANN advisory group to date. Our principal concerns remain the proposed voluntary nature of the program as regards its application to banking and financial services TLDs and the lack of commitment to establish such a program for use by applicants in this industry as an essential part of the launch of new gTLDs. More fundamentally, the 25 September 2010 ICANN Board statement that ICANN will not sponsor such a program is of grave concern to us as stated in the cover letter.