High Security Zone Top-Level Domain Advisory Group

Final Report

STATUS OF THIS DOCUMENT

This is the Final Report as developed by the community members participating in the High Security Zone Top-Level Domain (HSTLD) Advisory Group (the “Group”). The Group during the course of its deliberations did not reach consensus on a recommended approach to implementing a proposed HSTLD Program and thus this report serves to document their work and includes descriptions of the shared positions among its members.

Table of Contents

1.0 EXECUTIVE SUMMARY

The genesis of the High Security Zone TLD Advisory Group (the “Group”) can be traced back to the four overarching issues identified that needed to be addressed before the introduction of the new gTLD program, specifically Mitigating Malicious Conduct. In retrospect, a more appropriate name for the Group could have been the High Security and Trust Zone TLD Advisory Group because early in the process it became clear, based upon the Group's adopted "problem statement" and "goal statement", that this was a multi-disciplinary group (technical, legal, policy) whose primary focus was on enhancing the degree of trust over baseline controls within the domain name space. The “benefits statement” in Section 2.0 of this report highlights some of the intended effects of the proposed program for registries, registrars, registrants and users. Given the ambitious nature of this goal there were some within the Group that questioned the viability of its undertaking. However, rather than pre-ordaining the outcome or excluding any potential solutions, a full range of positions and options were available for discussion throughout the course of the Group's work.

The primary challenge for the Group was reconciling a number of diverse/divergent positions and proposals. On one end of the spectrum there was support for a mandatory "verification program" administered by a third-party auditor(s) for TLDs that require a high-confidence infrastructure or are at an unusually high risk for malicious conduct. In the mandatory Program, HSTLDs would have been required to publicly display a “verification” seal on their websites. At the other end of the spectrum was the belief that the problem and goal statements were never properly defined, and uncertainty about the incremental security and trust benefits that the proposed Program would bring to consumers. A third hybrid approach was offered which was a voluntary "report card" intended to be a compromise between the aforementioned proposals and to provide a foundation for future work within the community.

The chair attempted to facilitate and document the consensus development process within the Group based upon the Affirmation of Commitments’ principles:

- Engaging in "fact-based policy development";
- "Ensure that [the Group's] decisions are in the public interest, and not just the interests of a particular set of stakeholders";
- "Perform and publish analyses of the positive and negative effects of its decisions on the public"; and,
- "Provide a thorough and reasoned explanation of decisions taken, the rationale thereof, and the sources of data and information on which ICANN relied."

Notwithstanding adherence to these principles, the work of the Group as originally chartered has reached a point where additional work is unlikely to produce any more meaningful agreement among its participants. Therefore, it is proposed that this third report by the Group serve as its conclusion.

2.0 PROBLEM/GOAL/BENEFITS STATEMENTS

On 22 February 2010, the Group published its first Program Development Snapshot that provided a status report on their progress since its formation in January 2010. Included the report were consensus views on the Group’s problem, goal, and benefits statements. It was these three foundational elements that formed the basis for the Group's work and the draft control elements that were included in its second Program Development Snapshot published on 16 June 2010.

Problem Statement: The purpose of this statement was to document the issues the Group's work was intended to address as one of the measures to mitigate malicious conduct in new gTLDs.

> *"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."*

During the Group's early discussions of the various stakeholders that would have an interest in a high security top-level domain initiative, the following parties were identified:

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 Registrants and Registrars;
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; and,
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.

Goal Statement: The value of this statement was to provide the community with a charter of the overall goal of the Group. It provides a method of communicating the overall goal and direction to the community and to Group's members.

> *"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."*

Benefits Statement: The final foundational area of program development was to develop a Group benefits statement. The purpose for this statement was to help the community understand what benefits could be achieved through the adherence to an HSTLD Program.

> *Registries benefit:*
>
> *Ry1. by demonstrating that they have a high standard for continuity, security and operational integrity through some defined and reasonably consistent 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; and,

Ry6. that there would be some reasonable recurring term (annual/biannual) with review for continued affirmation of those standards remaining intact or improved.

Registrars benefit:

Rr1. by demonstrating that they have satisfied all standards for continuity, security and operational integrity that "trickle down" from an 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.; and,

Rr6. *that there would be some reasonable recurring term (annual/biannual) with review for continued affirmation of those standards remaining.*

Registrants benefit:

Re1. by demonstrating that they are willing to submit to a stringent verification measures associated with an 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 Terms of Service/Acceptable Use Policies 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.; and,

Re6. that there would be some reasonable recurring term (annual/biannual) with review for continued affirmation of those standards remaining

Users benefit:

U1. from more accurate registration data;
U2. from lower incidents of malicious registrations and DNS abuse among domain names registered in an HSTLD; and,
U3. from clearly defined abuse handling processes.

3.0 SUMMARY OF STATUS REPORTS

During the course of its work, the Group published two status reports for public comment to inform the community of its progress. The first snapshot was made available on 22 February 2010 as part of an ICANN announcement detailing the progress of some of the efforts underway to mitigate malicious conduct in new gTLDs. The second snapshot was published on 16 June 2010 in an ICANN announcement about new gTLD program materials that were available for public comment.

Snapshot #1

The purpose of the first report was to highlight the Group's work since its formation was announced on 3 December 2009. The development snapshot described the activities completed or in progress of the Group at that time. As noted in the announcement, the draft work in the document reflected the 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. Work presented in the report was considered a "work in progress." A public comment forum was opened on the report from 22 February 2010 through 8 April 2010, and the summary and analysis of the remarks received is provided in Section 7.0 of this report.

The Group's primary task during the initial stages of its work was to review the HSTLD Concept Paper that was published with the new gTLD draft Applicant Guidebook in October 2009. The paper introduced the concept for a program that would be designed to provide a structured approach to improving Internet community trust and to improve the overall security of the domains registered within TLDs that volunteer to participate in the program. In addition to the concept paper, an extensive list of background materials for consideration was provided to the Group on 12 January 2010 by Dave Piscitello, Senior Security Technologist at ICANN.

The primary outputs presented in the first report were the preliminary goal, problem and benefits statements noted in Section 2.0 of this report. Also introduced in this report were the "report card" concept, and a potential new method of reporting for the TLDs that are interested in becoming a HSTLD. The method would provide a mechanism for TLD's to self-certify their compliance with the HSTLD program. The Group did some limited evaluation (see Section 4.0 of this report for additional information) of this reporting method against other certifications, trust marks, and similar verification programs. Ultimately however, the Group found that while self-certification could provide limited benefits as part of a more extensive auditing and periodic-review program, it alone could not provide the level of assurance and accountability necessary to warrant HSTLD verification.

Finally, the first report contained draft principles, topics, objectives, and sample criteria that could serve as the foundation for the Group's work. Although consensus was not reached with regard to the four principles listed here, they are included for reference by any subsequent effort.

- 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, etc.) 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.

- 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.

- 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.

- 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.

Snapshot #2

In its second update to the community that was announced on 16 June 2010, the Group detailed the significant progress it had made in development of draft control standards that could be adopted by an HSTLD. A public comment forum was opened from 16 June 2010 through 21 July 2010, and the summary and analysis of the remarks are provided in Section 7.0 of this report.

The primary focus of the second report was to present the current framework of principles and criteria (the "Control Worksheet") that could form the basis for the core requirements of an HSTLD Program, and to share output from the HSTLD Survey. The Control Worksheet was the product of several months of work by the Group to develop illustrative controls to support the four principles identified in snapshot #1. In summary, the standards were categorized as principles (4), objectives (11) and criteria (57). The illustrative control activities were categorized as industry specific (100), draft Applicant Guidebook (28), Webtrust EV (34), Anti-Phishing Working Group (26) and International Organization for Standardization 27002 (119). In total, 307 illustrative controls were presented in the report. It is the example of a common framework that could allow TLDs interested in achieving designation as an HSTLD to demonstrate and uphold enhanced security-minded practices and policies.

The draft HSTLD Control Worksheet requirements, found in Appendix A to snapshot #2, were divided into two sections, “HSTLD Standards” and “HSTLD Illustrative Control Examples.” The section labeled “HSTLD Standards” contained the actual HSTLD Program core requirements and the section labeled “HSTLD illustrative Control Examples” provided sample control activities that a TLD might use, to meet the core requirements defined in the HSTLD Standards section. The HSTLD Standards section set out broad statements of principles, and then described a set of general control topics and objectives for each principle. Finally, a set of specific control criteria linked specific security objectives to the broad principle statements. The specific control criteria defined the benchmarks that were used to measure and present an HSTLD’s supporting control documentation, against which a qualified independent evaluator could evaluate compliance with the HSTLD Program.

Also provided in the second report were the results of the HSTLD Survey (see Appendix B to snapshot #2) that was conducted to take a point-in-time look at several issues that had been debated within the Group. As noted in the report, the issues had not been tested for consensus, and the survey was not representative of any agreement, consensus or decision. Highlights from the survey included:

- 81% support HSTLD should be a voluntary program;
- 50% support HSTLD should contain a certification program option;
- 25% support HSTLD should contain a report card option; and,
- 67% of those supporting a report card option said it should be supported by an external-audit function.

4.0 SUMMARY OF OUTREACH EFFORTS/FACT BASED RESEARCH

The information presented in Sections 4.1 to 4.8 is a description of how and with whom the Group conducted its outreach efforts and the results of those activities.

4.1 OVERVIEW/INTRODUCTION OF EFFORTS IN ACCORDANCE WITH THE AFFIRMATION OF COMMITMENTS (AOC)

This Group was constituted shortly after the execution of the Affirmation of Commitments (AoC) between ICANN and the United States Government. The Co-Chairs early on identified the AoC as a guiding document in how the Group would undertake their work and this was conveyed to both ICANN staff and the Group as a whole. Listed below are the specific principles from the AoC that the Group incorporated into its work and the result of that effort:

Paragraph 3 of the AoC states that “ICANN and the DoC commit to ensure that decisions made related to the global technical coordination of the DNS are made in the public interest and are accountable and transparent.”

The Group undertook an effort at the beginning of its work to ensure that any and all stakeholder holders had the ability to participate in the Group, at no time was membership restricted to new comers despite some early suggestions to close membership to the Group. All of the meetings except for the meeting with regard to confidential information in connection with the Request for Information were recorded and made available on the HSTLD website.

Paragraph 3 of the AoC states that "ICANN and the DoC preserve the security, stability and resiliency of the DNS"

While the Group included a multi-disciplinary group of participants, efforts were undertaken to make sure that representatives from Registry Operators community participated. Despite some early interest from some ccTLD registries, most of the registry participation involved the larger registry infrastructure providers such as VeriSign and Afilias. ICANN staff Dave Piscitello, Senior Security Technologist, also participated in various stages of the Group's work. While more technical specialists did not participate in the Group's work, the Registry Operators that did participate were able to provide feedback to the Group that was helpful.

Paragraph 4 of the AoC states that "ICANN and DOC recognize that there is a group of participants that engage in ICANN's processes to a greater extent than Internet users generally. To ensure that its decisions are in the public interest, and not just the interests of a particular set of stakeholders, ICANN commits to perform and publish analyses of the positive and negative effects of its decisions on the public, including any financial impact on the public, and the positive or negative impact (if any) on the systemic security, stability and resiliency of the DNS."

Because the Group did not make any specific decisions/action, it was unable engage in any detailed impact statement. Participating Registry Operators briefed the Group regarding potential operational and financial impacts of certain proposals. The Group would expect ICANN to provide a detailed analysis as required by the AoC if it undertakes unilateral action in connection with this initiative to tick the Mitigating Malicious Conduct box to move forward with the new gTLD initiative.

Paragraph 7 of the AoC states that "ICANN commits to …. fact-based policy development."

The Group undertook a number of fact based initiatives to guide its work including: review of relevant Security and Stability Advisory Committee (SSAC) reports identified by Dave Piscitello; briefing material provided by BITS on behalf of the financial services community; contributions from Registry Operators and other security experts during the controls drafting exercise; a briefing from TrustE about different options to increase consumer trust; as well as a Request for Information process that included written submissions as well as a telephone questions and answers session.

Paragraph 8 of the AoC states that "ICANN affirms its commitments to … operate as a multi-stakeholder, private sector led organization."

There were some concerns expressed during the Group's deliberations regarding the lack of "technical" expert contributions and a limited number of participants at different times during the work. However, the Group remained open to anyone wishing to participate, and that the core group of members that contributed did represent a fairly broad range of the multi-stakeholders within the broader ICANN/Internet community.

4.2 SUMMARY OF CALLS, NUMBER OF PARTICIPANTS, STATEMENTS OF INTEREST

The Group was formed in December 2009 after an ICANN announcement on 3 December 2009 soliciting volunteers to work on a temporary expert Advisory Group to study and develop a proposed solution for establishing a high security TLD verification program. The Group convened its kick-off meeting on 15 December 2009, and as of 23 December 2009, was reported to have 31 volunteers. Statements of Interest for the members are viewable at the HSTLD public wiki.

From 15 December 2009 through 7 March 2011, the Group convened 47 conference calls and the mp3 recordings from these sessions are available at the HSTLD information web page. This page includes a record of the calls and papers produced by the Group as well as the link to the public archive of its mailing list.

The primary contributing authors to this Final Report include: Michael Palage, Mikey O'Connor, Paul Smocer, John McElwaine, Lynn Goodendorf, Pam Dicioccio, Eric Brunner-Williams, Jothan Frakes, and ICANN Staff including Craig Schwartz and Dave Piscitello.

4.3 ORIGINAL BITS PAPER/CONSULTATION WITH ICANN

In early 2009, representatives from four major financial industry associations met with Kurt Pritz, then ICANN's Senior Vice President, Services and Greg Rattray, then ICANN's Chief Internet Security Advisor. The four associations were the American Bankers' Association (ABA), BITS (a division of the Financial Services Roundtable), the Financial Services – Information and Analysis Sharing Center (FS-ISAC), and the Financial Services Technology Consortium (FSTC).

The stimuli for the meetings were comments made in both the ABA's and BITS' responses to draft Applicant Guidebook v1. While at that time the associations had concerns regarding a number of areas including cost/benefit, trademark protections, and scalability, the focus of the discussions was on concerns both associations had raised regarding the need for protection of users of domains whose primary purpose is to offer financial services and the associated needs of security and prevention of malicious conduct.

Because of these meetings, on June 21, 2009, then ICANN President and CEO Paul Twomey sent a letter to the four associations with an offer to engage the sector by asking them to develop more detailed requirements regarding security, stability, and resiliency. The four associations worked collaboratively and reached out to a number of other organizations for input. These other organizations included the associations' member companies, several non-U.S. financial services trade associations, and select experts.

The associations' effort at the time actually concentrated on two objectives. The first was to identify potential process changes within the Applicant Guidebook that would allow ICANN and the sector to both identify and evaluate applications for new gTLDs where their use was primarily for offering financial services. The results of work on that objective are now dated (due to multiple changes in the draft Applicant Guidebook since that time), and are not germane to the work of the HSTLD. What is relevant to the Group's work are the outcomes of the associations' second objective. The second objective was to identify a set of security, stability and resiliency requirements for TLDs whose primary purpose is to offer financial services. Based on our discussions with Greg Rattray, we tried to keep these requirements at a higher level rather than a very detailed level. On August 6, 2009, the associations submitted the results of its work to ICANN in a letter addressed to Rod Beckstrom, who by then had become ICANN's President and CEO. The letter, including its attachments specifying the associations' recommended security, stability and resiliency requirements for financial TLDs is available at http://www.bitsinfo.org/downloads/Comment%20letters/BITSCommentLetterICANNgTLDProcessRequirements080609.pdf.

The Group discussed and considered whether other additional industry sectors might have a similar interest. The conclusion was that there is a high probability of interested parties other than financial services. The view is that those who are high profile targets for fraudulent and domain abuse activities would be potential stakeholders. But in the interest of progressing work in a timely manner, this point was not researched. The Group recommends that future work related to this concept include a survey or outreach effort to identify other interested parties with similar concerns.

4.4 BACKGROUND ON REQUEST FOR INFORMATION (RFI)

Following the publication of its second status report, the Group determined that issuing a Request for Information (RFI) could be an effective method to gather more information about how an HSTLD program could be developed and implemented. On 22 September 2010, ICANN and the AG announced the publication of the RFI.

The purpose of the RFI was to assist the ICANN community in collecting data from prospective contractors and other interested parties that have experience in designing and working with other popular control and security verification programs in the USA and internationally. The Group reached out to well-known standards development organizations, auditing/attestation firms and other companies that specialize in issuing certifications, trust marks, and seals to facilitate a broad range of responses to the RFI.

In addition to providing an overview of the Group's work-to-date, the RFI contained 12 questions that solicited information on the respondents':

- Experience with ICANN or entities that interact with ICANN;
- Experiences with security mechanisms, controls, auditing, or similar activities;
- Assessment of HSTLD Program requirements and potential assessment mechanisms;
- Advice on potential implementations;
- Data on potential costs for registries, registrars/resellers, and registrants;
- Assessment of the HSTLD Control Worksheet Criteria Objectives; and,

- Timeline estimates to implement an HSTLD Program.

The RFI response period was open from 22 September 2010 to 17 December 2010, and a summary of the Group's interactions with potential respondents and the responses received are provided in Section 4.5 of this report.

4.5 SUMMARY OF CALLS WITH INTERESTED PARTIES

Following the publication of the RFI, the Group convened several calls with interested parties and potential respondents to respond to questions about the RFI and to provide clarification about the HSTLD Program. The Group received 30 questions about the RFI from the period 22 September 2010 through 27 October 2010. The questions along with their answers may be viewed here.

On 23 November 2010, the Group invited those organizations who submitted questions on the RFI to participate in a conference call to discuss the answers that had been provided to them and to potentially respond to other questions they might have. The following organizations participated in the call: Deloitte & Touche, Ernst & Young, KMPG, Grant Thornton, PricewaterhouseCoopers, NetChoice, and Symantec. The mp3 recording and unofficial transcript from the call are available on the HSTLD Information web page.

The HSTLD topics discussed in the greatest detail were: program sponsorship; program controls and structure; and auditing/attestation services providers and their ability to participate in an HSTLD Program.

There was consensus among those on the call that ownership or administration of the HSTLD Program or some other verification process, including issuance of a seal, should rest with ICANN. Group members and call participants agreed that ICANN's role in a verification program is important for the global perception of and instilling confidence in the value of the HSTLD designation. The concept that ICANN should maintain some form of ownership of the HSTLD Program's controls is consistent across members of the Group and call participants. Several respondents commented that it will be difficult to identify a third-party provider(s) without a clear understanding of the demand for the service and the return on investment for potential providers. Michael Palage, Chairman of the Group, suggested that HSTLD could perhaps be operated similarly to ICANN's Uniform Domain Name Dispute Resolution Policy (UDRP) where the process is developed and maintained by ICANN, but administered by ICANN-accredited providers. Lessons learned and a recommendation about the Group's work on the HSTLD Program are been provided in Sections 8.0 and 9.0 of this report.

A significant portion of the call was spent discussing the draft control standards and the challenges of implementing them in a verification program. Respondents noted that highly specific controls would likely be more onerous and costly to implement through the value chain of the domain name registration process. On the other hand, it was further noted that the more general the controls are the more important it is to ensure the qualifications of the validation service providers meet pre-determined standards. Lastly, and discussed in more detail below, is that Certified Public Accountant (CPA) auditing/attestation firms are bound by the American Institute of Certified Public

Accountants (AICPA) with regard to what they may audit, the forms of report they may provide, and the seals they may issue. As such, program criteria and structures that do not meet these standards could have a negative effect on the implementibility of an HSTLD Program and would certainly limit participation by such firms.

Perhaps equally important to the control standards discussion was that of an auditing/attestation firm's ability to provide their service to TLDs who might seek HSTLD verification. As noted above, CPA firms are bound to principles defined by the AICPA relating to the objectivity, measurability, and suitability of criteria or control standards. All participants suggested that while they could not administer the HSTLD Program due to AICPA regulations, they could provide their services if the controls and program structure comply with the prescribed standards. The HSTLD Program currently defines 307 control mechanisms which several cited as being far too many. Additionally, these control standards in their current form do not comply with AICPA standards.

In summary, respondents indicated an interest in continuing to be helpful in the evolution of the HSTLD Program and several stated they could assist ICANN in developing the administration model. However, more work needs to be done in the areas of: defining the intended outcomes of a Program should one be instituted; determining ownership and ongoing administration of the Program and the controls; reducing or at a minimum modifying the current set of control standards to be more objective and measurable; and, defining how the Program might be applied across the value chain of participants in the domain name registration process.

4.6 SUMMARY OF CALL WITH TRUSTe

On 15 December 2010, the Group hosted a call with representatives from TRUSTe, a privacy certification company which utilizes a combination of skilled expertise, technological tools, and reputation management tools to provide transparency, accountability and choice services for websites, applications and advertisers. Additional information about TRUSTe can be found at www.truste.com.

Prior to this call, TRUSTe advised the Group that they would not to respond to the RFI because they felt it was heavily focused on a security audit approach and that is not their core competency. However, TRUSTe representatives did offer to participate in a call with the Group to share their expertise in managing a large privacy and reputation data and services infrastructure to help consumers and businesses trust online transactions and requests for personal information. The primary mechanism for attesting to this certification is by use of a website trustmark or seal which provides an indicator that a company complies with TRUSTe's program requirements.

Unlike the 23 November 2010 conference call with interested parties, the discussion with TRUSTe was not recorded due to technical issues and the summary provided below has been validated for accuracy by TRUSTe.

Key Discussion Points

- The overall goal for this type of program is usually about promoting trust and confidence. Who is the target audience for promoting trust? Is it the registrant in making a choice of registrars? Or is it Internet users across the general public? What is the threat model ICANN wishes to protect or enhance?

- The question of cost justification was raised. As a voluntary program, it needs to be financially viable in terms of a benefit/cost analysis for a gTLD Registry Operator or registrar to participate. Similarly, further work is indicated to develop cost estimates for ICANN to consider.

- Concerns about liability for ICANN could be addressed in the detailed design of the program.

- A key question is whether ICANN would want to establish a “standard” that is applicable specifically for the domain registration space.

- The scope of controls currently drafted is broad and deep. If the Program is further defined as a trust model, TRUSTe would be in a position to narrow the scope of the standards.

- TRUSTe has a “watchdog” program that provides a feedback loop for Internet users. This reinforces accountability with the web seal holders who agree to process and procedure of the watchdog program as part of the program. This is an element we have not yet considered in the design of an HSTLD program.

Note: Participants that undergo the process of TRUSTe privacy certification program are provided a seal as a visual indication of participation in the program.

There have been discussions within the Group that raised the concept of a labeling ‘seal’ for a registry that would have undergone a successful audit. The point was made that a seal display for HSTLD, similar to the ICANN-accredited registrar logo, could positively impact the confidence and trust registrants and end users have in the TLD. Additionally, it was discussed that a seal that does not incorporate ICANN’s logo or name would be of less benefit.

4.7 SUMMARY OF RFI RESPONSES

In response to the RFI posted on 22 September 2010, the Group received submissions from KPMG, Deloitte & Touche, BITS, and Toegepast Natuurwetenschappelijk Onderzoek (TNO). All of the firms except TNO participated in the 23 November 2010 conference call summarized in Section 4.5 of this paper and their submissions closely mirror remarks they made to the Group on the call.

In their respective responses, the firms demonstrated an understanding of ICANN and the domain name industry based upon their experience either directly with ICANN or entities within the ICANN community such as gTLD and ccTLD registries and ICANN-accredited registrars. KPMG and Deloitte & Touche cited their obligations under AICPA guidelines, operational knowledge of the International Organization for Standardization (ISO) 27000 series for information security management, and SysTrust and WebTrust for Certification Authorities.

The BITS response acknowledged that they would not be an implementing organization of an HSTLD Program and thus their submission did not contain details comparable to that from the other respondents. BITS responded to the RFI to voice their support of the Program and to reaffirm their position that such a Program should be mandatory before applications for new gTLDs principally focused on providing banking and financial services are accepted.

KPMG and Deloitte & Touche are well-known, international consultancies that at one time or another have done work for ICANN and or its contracted parties. Their responses presented similar information which on some level was to be expected as they both are required to conform to AICPA guidelines. For example, both firms identified:

- A range of options for assessing an applicant's compliance with the HSTLD Program requirement as well as their respect advantages and disadvantages. A presentation of the options is provided below in the "Highlights" section of each response;
- The need to review and revise control standards/criteria to conform to audit/attestation principles of completeness, measurability, objectivity and relevance;
- The estimated time to develop and implement a Program could be on the order of 12 months depending on the final requirements;
- The value of ICANN administering the Program, retaining some oversight of the control standards, and issuing the certification, trust mark or seal; and,
- How assessment activities could be distributed across the domain name value chain.

KPMG Highlights

KPMG devoted significant attention to presenting assessment options and their pros and cons. Following is a brief summary:

- Self-assessment
    - Pros - easiest to implement, more cost effective for applicants, and provides guidance to applicants on best practices
    - Con - least amount of assurance
- Independent Audit (after audit process is developed)
    - Pros – greater level of assurance, and some existing frameworks (e.g., AICPA standards) can be leveraged to mitigate impacts to ICANN and HSTLD applicants
    - Con - challenging to implement and more costly to applicants
- Hybrid approach – initial independent audit/review followed by a period of self-certification
    - Pros - enhanced level of assurance and alternative to mitigate costs for registries and registrars
- KPMG recommended an audit approach to include periodic assessments with a one-year period of coverage; this provides greater assurance of compliance than a point-in-time assessment.
- With regard to the domain name value chain, assessment would need to be expanded to registrars and resellers through their contractual obligations with registry operators. Registry operators could also periodically monitor registrar and reseller activities and the third-party assessor could test the effectiveness of

the registry's controls. It was noted that cost considerations of such a process may figure prominently in whether a registry elects to adopt HSTLD.

- Registrant verification is an important element of the registry operator's registration process.
- SAS 70, WebTrust and SysTrust, depending on complexity, can range from $25k to $1M. Potential cost is difficult to estimate given a number of factors including time covered, level of assurance required, complexity of the domain name chain, complexity of the environment, readiness of the TLD to be audited, etc.
- Status (i.e., certificates, trust marks, seals, etc.)
    - Demonstrates commitment to high security
    - Some factors for consideration include:
        1. Who issues, administers and maintains status?
        2. Does status link to a report?
        3. How could the status be revoked and the revocation enforced?

Deloitte & Touche Highlights

Deloitte provided an overview of several assessment program options and substantial details regarding implementing various assurance engagements.

- Critical Success Factors:
    - Establish level of trust necessary for all participants in the process. Necessary to look beyond registries in order for registrants and users to have a more complete view of security risks and controls within the TLD;
    - Establishment of relevant, complete, neutral, measurable and understandable criteria;
    - Consistent assessment and reporting standards be employed globally;
    - Properly qualified assessors;
    - Trust seal should link to the report that underlies the seal, mark, etc.;
    - Pricing model for sustainability needs to be established; and,
    - Engage a firm to develop and participate in the audit/assessment process.
- Assessment Options:
    - Audit – done under Generally Accepted Auditing Standards (GAAS), will produce the highest level of trust, will be the most costly (e.g., WebTrust for Certification Authority (CA) and Extended Validation (EV) programs);
    - Review – addresses the plausibility of controls meeting particular criteria. Currently not permitted in assurance standards in North America and not being used internationally;
    - Specific procedures engagement – assessor performs certain assessment procedures that were agreed to in advance. Restricted report is produced and users draw their own conclusions (e.g., Payment Card Industry (PCI) assessment); and,
    - Assessment consulting engagement – consultant provides observations on whether certain controls have been designed and implemented properly.
- Certification Schemes
    - For trust, the scheme should be open, transparent, and capable of consistent measurement. Ideally all liability for reliance on any seal should rest with the applicant, not ICANN;

    - Auditing firms are accredited via license; responsibilities and liabilities are defined in the license. The auditing firm arranges for the seal, not the issuing entity and the seal links to the audit report; and,
    - Sometimes determination about whether to issue a seal is done by the issuing entity rather than the auditing entity.
- The determination regarding the level of assurance required will drive the certificate scheme.
- Popular controls and compliance programs
    - Level of assurance: higher levels provide more trust;
    - Ability to self-assess: does not provide any level of assurance or trust;
    - Frequency of audit/assessment: annual audit is a sound approach;
    - Compliance framework/audit criteria set: The recommendation was that the program favor principles, criteria and illustrative controls rather than prescriptive standards;
    - On-site assessment: important when technique requires observation and provides better value to clients;
    - Share report with public: important in providing trust;
    - International participation: important if program wishes to be accepted worldwide;
    - Oversight body: important to monitor the success of program and update the program to reflect the changing needs of stakeholders;
    - Communicating audit results: seal, watermark, report cards help public realize effort that's gone into the maintenance of controls;
    - Assessor must be qualified: improves quality of results and integrity of program;
    - Assessor organization or employer must be qualified: improves quality of results and the integrity of program; and,
    - Levels of compliance: can facilitate gradual adoption of program, but change can be complex to manage and explain.
- Proposed assessment program: point-in-time and periodic assessments of the registry operator – greatest flexibility, reasonable timelines, and a high level of assurance. Steps of the process are:
    - Initial Self-Assessment: documentation and evidence uploaded to secure portal – helps drive audit costs lower if registry is doing more of the document and evidence preparation.
    - HSTLD Readiness Assessment: point-in-time audit to test design and implementation of technical and procedural controls. Output is a controls gap report and risk rating accompanied by a remediation plan that must be auditor approved.
    - Remediation: should occur within one year or the full readiness assessment should be conducted again:
        1. Upon completion of remediation of identified high or critical control gaps, start operating effectiveness period; OR
        2. Same as 1 plus point-in-time readiness report can be issued and one with an unqualified audit opinion would warrant issuance of the HSTLD seal.
    - Operative Effectiveness Period – If 1 above, audit should be between 2 and 12 months. If 2 above, no greater than 12 months.
    - HSTLD Audit: conducted as a period of time audit to test the design, implementation and operating effectiveness of the technical and

    - procedural controls. At this point seal would be issued or re-issued for 12 months.
    - Self-Assessment Renewal: update self-assessment with results from the HSTLD audit.
- Assurance engagements and assurance based reports
    - Deloitte recommends an audit level or high assurance program be mandated to provide a higher level of trust.
    - Practitioner is engaged to:
        1. Issue an opinion (examination/audit); or,
        2. Conduct a review; or,
        3. Conduct agreed upon procedures.
    - Professional auditing and assurance standards must be followed.
- Engagement types
    - Examination/audit: high though not absolute level of assurance (e.g., WebTrust for CA).
    - Review: moderate level of assurance (difficult to assess what moderate is).
    - Agreed-Upon (Specified Auditing): performs specified procedures and reports findings. No audit with this type. Not ideal since user's needs vary wildly.
    - Comparison to Current Payment Card Industry Data Security Standard (PCI DSS) Reporting: performed by quality security assessors, rather than by CPAs or their equivalents. Drawbacks to this approach include:
        1. Auditing standards can be modified by report users to accommodate e.g., environment specifics. Attestation/assurance frameworks are not; and,
        2. DSS does not provide an opinion in accordance with recognized auditing standards.
- How assessment is supported by registrar and reseller operations
    - Service audit reports: sub-service organization may contribute to achievement of control objects.
    - Assessment could be done against specific controls and criteria.
- Considerations for expanding verification beyond registry operations:
    - Registry Operator builds in a right to audit clause into contracts with their registrars;
    - Carve out controls which require assessment/audit of registrars;
    - Build an extension to assessment program specifically for registrars; and,
    - Benefits to registrars; basis for differentiation in the marketplace.
- Costs are largely dependent on assessment/assurance model selected.
    - Registries: Readiness assessment $30-$50k, operating effectiveness assessment $40-$60k plus cost of seal maintenance (est. $2500)
    - Registrars: Readiness assessment $10-$15k, operating assessment $10-$15k plus cost of seal ($500)
- Suitable audit criteria must meet standards of the Framework for International Standards on Assurance Engagements:
    - Relevance
    - Completeness
    - Reliability
    - Neutrality
    - Understandability

- Time to implement the program: 10-12 months
- Publicly representing verification status
  - Scorecards are generally misunderstood by the marketplace
  - No accepted guidelines published for scorecard reporting
  - Issues with seals:
    1. Public education about seal, what does it mean, what does it not guarantee (public education is costly);
    2. Management of seal process to protect integrity;
    3. Determining right value of seal; and,
    4. Secure reporting.

TNO is an independent Information and Communications Technology (ICT) auditing and certification organization and security of ICT is one of their areas of expertise. TNO remarked that the intention behind the HSTLD Program needs to be clarified before additional work is undertaken to ensure that what is developed is consistent with the desired outcomes of the Program. Their response primarily focused on how they would assess and audit registries and they noted it would be similar to ISO certifications as the HSTLD controls in many cases mirror ISO standards.

<u>TNO Highlights</u>

- Assessments/Audits
  - Full – conducted once every four years or longer
  - Re-assessments – less extensive and conducted once every two years between full assessments/audits
  - New TLDs – frequency could initially be higher until maturity in operations
  - Should be tailored for each registry depending on type and size
- Multi-level program
  - Basic security level based on current best practices of leading registries
  - High security level to include continuous external monitoring in addition to regular assessments/audits
    1. Benefit – insight to the actual security level as experienced by external users
- Measurement framework for security
  - Integrity – biggest challenge is anomaly detection
  - Availability – straightforward, though volume of data is a consideration
  - Confidentiality – less important since DNS data is public information
- Assessment considerations for registrar or reseller operations
  - Achieved through verification of a Service Level Agreement (SLA)
  - Numbers of registrars or resellers will inform approach to assessment
- Value Chain of Trust
  - Program objectives should be realistic
  - HSTLD concept as written may raise false expectations about the security spectrum from registry to registrant
  - Assessment/auditing level may need to be different for registries and registrars
- Costs for Registries: Full $40-$70k, re-assessments $20-$35k
- Control Worksheet Criteria
  - One size does not fit all; all criteria will not be relevant for each registry
  - Should be refined after experience from the first HSTLD audits

- Time to implement (basic level) is 6-12 months.
- Publicly representing verification status
  - Could raise false expectations; seals may get misinterpreted by the community that TLD is “safe”
  - Seals can create a tool for abuse and thus require policing
  - Public auditing report is favored deliverable from an audit

4.8 CONCLUSIONS FROM OUTREACH

Summary of Conclusions from Outreach		
Objective: Solicit information from industry experts on frameworks for evaluating new gTDS against the proposed HSTLD Program		
Method of Gathering Data	**Participants**	**Summary**
RFI Solicitation	• Standards firms • Security firms • Auditing/Attestation firms • Cert/Trust Mark/Seal firms	• Ownership or administration of the HSTLD Program or some other verification process, including issuance of a seal, should rest with ICANN; • CPA firms cannot administer the HSTLD program as criteria would have to comply with American Institute of Certified Public Accountants (AICPA) regulations in order for CPA firms to participate; and, • 307 control mechanisms are far too many controls, and in their current form they do not comply with AICPA standards
RFI Question/Response Call (Nov 23, 2010)	• Deloitte & Touche • Ernst & Young • KMPG • Grant Thornton • PricewaterhouseCoopers • NetChoice • Symantec	
RFI Response	• KMPG • Deloitte & Touche • Toegepast Natuurwetenschappelijk Onderzoek (TNO) • BITS	• Establish level of trust necessary for all participants in the process. Necessary to look beyond registries in order for registrants and users to have a more complete view of security risks and controls within the TLD; • Establishment of relevant, complete, neutral, measurable and understandable criteria; • Properly qualified assessors are needed; • Trust seal should link to the report that underlies the seal, mark, etc.; • Pricing model for sustainability needs to be established; • A firm should be engaged to develop and participate in the audit/assessment process; • Time to implement an assessment program: ~12 months; and, • Proposed assessment program: point-in-time and periodic assessments – creates greatest flexibility, reasonable timelines and a high level of assurance.

5.0 COMPARABLE MODELS AND METRICS

The purpose of the Group was 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." The form of such voluntary program to provide an enhanced level of trust and security could be accomplished in many ways such as a certification or trust mark, a scorecard, or a self-assessment metric, among other methods. During the Group's meetings with relevant community members, it became apparent that there is no interest amongst ICANN or the relevant community to implement a certification program at this time.

What follows below is Table 5.1 that was created by Deloitte & Touche LLP and submitted in their RFI response.

Table 5.1 was submitted to address question three of the HSTLD RFI: How would you propose both point-in-time assessments of a TLD registry operator based on the HSTLD Program requirements and assessment methods described in the referenced concept paper? Deloitte's chart identifies issues that should be considered in the implementation of any trust or high (or higher) security program if adopted.

The issues identified in Table 5.1 may provide a roadmap of items to be discussed and vetted in developing a potential compliance program. In particular, the Group charged with implementation should take the following into consideration:

1) What statements of assurance will be provided in connection with the HSTLD assessment?
2) Should applicants have the ability to self-assess all or party of the controls?
3) If compliance with other certifications is accepted what diligence should of such certification should be undertaken?
4) Should ICANN have a minimum frequency of audit/assessment?
5) Should ICANN mandate audit/assessment standards?
6) Should ICANN require that audits be made available to the public?
7) Should ICANN approve or authorize assessors?
8) Who should create, review, and revise the underlying (DNS) standards?

Please note that the views and positions presented in the table are those of Deloitte. In addition, it is important to note that Deloitte's views with regard to the level of assurance of the assessment programs it enumerates (i.e., Web Trust for CA/EV, PCI DSS compliance program, the HiTrust program, and ISO Certification) are not shared by all members of the Advisory Group.

Two examples of where some in the Group deviated from Deloitte's view are the level of assurance for ISO Certification and the PCI Compliance Program. In the former, Deloitte indicated a "Low" level of assurance and in the latter "None." Certain security experts in the Group commented that because ISO Certification standards have been developed with a global consensus process engaging more than 30 countries and that organizations have latitude in developing a risk analysis and associated security objectives, there is at least a moderate level of assurance.

Certain members of the Group felt there is a level of assurance with the PCI Compliance Program, albeit the assurance is limited to confidentiality of credit card data, consistent with the overall goal of the PCI program (to mitigate financial losses related to credit card fraud). Completion of the program assures credit card merchants and processors will not be liable for contractual penalties but does not provide high level of assurance related to risk of data breach or loss.

Table 5.1 – Comparison of popular controls and compliance programs

Program aspect	WebTrust for CA/EV Program	PCI Compliance Program	HiTrust	ISO Certification	Considerations for HSTLD
Level of assurance given concerning controls at completion of the program	High level of assurance	None	High level of assurance for Common Security Framework ("CSF") Certified assessments. Lower level of assurance for CSF Validated assessments.	Low level assurance. Organizations can be certified by promising to fix control issues.	Higher levels of assurance provide a higher level trust. This is a key element in the criteria and objectives of the security verification program
Ability to self assess	No	Depends on merchant level based on number of transactions	Yes, but only a lower level of assurance can be provided via self assessment through CSF Validated assessments.	Self assessment is a part of ISO certification. Requires that management systematically examine the organization's information security risks, taking account of the threats, vulnerabilities and impacts. Ultimately to be certified a third party ISO assessor must review operations.	Self assessment can help an organization with expectations, but does not provide any level of assurance or trust with the general public

Program aspect	WebTrust for CA/EV Program	PCI Compliance Program	HiTrust	ISO Certification	Considerations for HSTLD
Frequency of audit / assessment	Annual	Annual	Review normally required annually. Re-assessment required every two years at a minimum.	Annual – often more frequently after initial certification	A lot can change in the course of 12 months – an annual audit helps management to prioritize focus on maintaining their controls
Compliance framework or audit criteria set	Yes - Principles, criteria and illustrative controls	Yes - control objectives linked to PCI DSS requirements	Yes – Common set of controls, questionnaires, assessment and reporting processes	A framework exists, however audit criteria for high assurance level reports have never been standardized.	One of the difficulties with applying the PCI standards is that they are very prescriptive. The use of principles, criteria and illustrative controls allows the framework to be intelligently fit the organization

Program aspect	WebTrust for CA/EV Program	PCI Compliance Program	HiTrust	ISO Certification	Considerations for HSTLD
Requires an on-site assessment	Yes	Depends on merchant level based on number of transactions	Yes, CSF Certified assessments require on-site assessment	Yes	On-site assessments are important when the assessment technique requires observation. Better value to the client is provided through on-site assessments
Report can be shared with general public	Yes	No	Yes, report can be distributed to external parties by organization depending on subscription level	Yes – ISO certification can be shared with public	Disclosure to the public is important in providing trust
International participation	Yes	Yes	Yes	Yes	International participation in developing the requirements is important for any program that wishes to be accepted worldwide

Program aspect	WebTrust for CA/EV Program	PCI Compliance Program	HiTrust	ISO Certification	Considerations for HSTLD
Oversight body	AICPA and CICA Electronic Commerce Assurance Task Force	Payment Card Industry Security Standards Council (PCI SSC)	HITRUST LLC and HITRUST Services Corporation	International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)	Oversight bodies are important to continuously monitor the success of the program and the needs of the stakeholders for which the program is directed make changes when necessary
How are audit results communicated?	Seal with audit report	QSA report to acquirer	CSF Certified certificate granted by HITRUST based on testing results of CSF assessor with specific year criteria of HITRUST noted.	Certificate	A seal, watermark or report card systems helps public stakeholders realize the value of the efforts that the attaining organization has put into maintaining controls
Assessor must be qualified?	Yes	Yes	Yes	Yes	Qualified assessors improve the quality of the results and the integrity of the program.

Program aspect	WebTrust for CA/EV Program	PCI Compliance Program	HiTrust	ISO Certification	Considerations for HSTLD
Assessor's organization or employer must be qualified	Yes - through a licensing system	Yes - must be approved by PCI Security Standards Council	Yes – must meet certain criteria and be approved by HITRUST	Yes, must be accredited	Qualified assessor organizations improve the quality of the results and the integrity of the program and are in the position to provide a more holistic value proposition to followers of the program
Different levels of compliance?	No	No	Yes, CSF Certified assessments and CSF Validated assessments provide different levels of assurance.	There are different stages of certification	Having different levels of compliance can facilitate gradual adoption but, on the other hand, add to the complexity to manage and can be more difficult to explain to users

6.0 RANGE OF POSITIONS CONSIDERED BY THE GROUP

One can consider the range of positions considered by the Group in two categories. The first category is the positions related to the nature of the Program and how broadly to apply an HSTLD Program (i.e., registry, registrar, reseller, registrant, and end-users, etc.). The second category relates to options regarding how to gauge the effectiveness of the application of HSTLD requirements in domains that choose to designate themselves as HSTLD compliant.

POSITIONS WITH REGARD TO THE NATURE AND BREADTH OF AN HSTLD

There were primarily four positions advanced by participants in the Group:

- Position #1 - A program conceptually similar to HSTLD has value, but at best should be fully voluntary. The arguments for this position included:
  - To force TLDs to comply can be very costly – particularly for smaller TLDs; and,
  - Not all TLDs necessarily need or require higher security or trust.

- Position #2 - A program conceptually similar to HSTLD has value, and should be required for some TLDs requiring "higher" trust, but voluntary for all others. The Group generally envisioned these as TLDs requiring high-confidence infrastructure or ones that are at an unusually high risk for malicious conduct. The basis for this position included:
  - Certain TLDs whose primary functionality involves the need for fundamental security (e.g., financial transactions, movement of funds, availability of non-public, private information, sensitive health care information) require a higher level of security and trust.

- Position #3 – There is no need for a program conceptually similar to HSTLD. The arguments for this position included:
  - Existing ICANN requirements mitigate the need;
  - It is difficult at best to judge whether a TLD effectively meets the requirements that would be defined within such a program;
  - Even if it were possible to judge compliance to the standards of such a program, the judgment is generally a point-in-time judgment that may not reflect current state; and,
  - Even if a robust set of standards exists and can be judged on some ongoing basis, it does not guarantee safety or trust. (An example of this concept was the current requirements of PCI and the breach at the ostensibly PCI-compliant Heartland.).

- Position #4 – The nature (and value) of a program such as HSTLD cannot be determined due to gaps in the analysis conducted by the Group. The basis for this position focus on the lack of consensus around a number of key issues, including but not limited to:
  - What problem would the HSTLD designation solve and for whom?;

- Who would be subject to HSTLD requirements – which combination of registries, registrars, registrants and end users?;
- What would be the change in operational feasibility if there is a dramatic increase in the number of TLDs given that this is likely to be a voluntary program?;
- What methods would be used to ensure actual operational effectiveness of the program?; and,
- How can feasibility of the program be determined, given the lack of consensus around the preceding points?

There was an additional position that the Group discussed early, though arguably it never truly considered. That position was "a program conceptually similar to HSTLD has value, and should be required by all." While some discussed the theoretical benefits of requiring all TLDs to be more secure, there was no strong support for this position and the Group dropped discussion.

POSTIONS WITH REGARD TO DETERMINING THE EFFECTIVENESS OF AN HSTLD PROGRAM

The Group was also divided between two major positions regarding the approach to ensuring actual operational effectiveness of the program.

- Position #1 – Operational effectiveness of an HSTLD Program can be ensured through the use of periodic external validation by external parties.

- Position #2 – The value and nature of external validation cannot be determined given the gaps in the analysis conducted by the Group (see Position #4 above).

The Group was not able to arrive at a consensus view that reconciled these two positions.

Members of the group who subscribed to Position #1 were, in addition, divided between two approaches to delivering that validation.

One can generally define "validation" as the set of methodologies used by a TLD to confirm to external parties its compliance to the standards set forth within the HSTLD Program. The Group's discussions covered various options in this area.

To assist its deliberations, the Group solicited input from various external parties with expertise in validation/ certification programs. (See section 4.7 Summary of RFI Responses for information on the solicitation processes and the outcomes of the RFIs received.) In the context of the debate around scope positions, the Group also debated whether any validation program was necessary or should be defined until some decision regarding moving forward with the overall HSTLD Program. Ultimately, the Group's discussions in this area focused on two key methodologies – formal verification and report carding.

- Formal Verification

  In this methodology, a TLD would be required to engage an independent third-party to audit and confirm its compliance with the defined requirements of the HSTLD Program. The Group's vision was that upon the third-party's conclusion that a TLD was compliant; the TLD would publicly display a “verification” seal on its website. The overall advantages of this approach are:

  - It provides an independent validation of compliance (thus increasing the trust parties relying on the validation can have);
  - It is largely consistent with concepts applicable to other validation programs in the IT environment (e.g., PCI) which makes it more understandable within the IT community and, to some extent, more acceptable to “consuming” parties; and,
  - Third-party servicers exist that could, and would be willing, to provide the services necessary to validate TLDs.

The overall disadvantages include:

  - Formal verification presents potentially significant costs associated with the employ of independent third-party assessors. Ancillary to the high cost issue is the question of how to allocate these costs across the various constituencies involved in the process (e.g., TLD owner, registries, ICANN); and,
  - There was discussion regarding the potential liabilities that a formal verification program might create. Liability arguably arises from two sources. First, from the reliance that outside parties likely would place on the accuracy of the attestation/verification process and the outcomes if that verification proved inappropriate. Second, from confusion by outside parties regarding to what attestation applies in a situation where an issue might arise that is outside of the bounds of what the HSTLD verification itself entails.

- Scorecard

  In this methodology, presented in draft form in Annex A to this report, the Program would create a mechanism for TLDs to self-certify their compliance with HSTLD Program. The self-certification would result in a scorecard that would provide information to interested parties of the level of compliance of the TLD to the HSTLD Program’s standards.

  This methodology is a compromise between a mandatory, third-party reviewer approach as defined under “Formal Verification” and the choice not to define any position regarding validation. The Group generally viewed it as an opportunity to provide an option that would provide a foundation for future work within the community. The ICANN Board’s decision not to support the HSTLD Program formally due to its concerns over liability also served as a stimulus for surfacing this alternative, as did the inability to reach consensus agreement within the Group during recent discussions to support a more formal option.

  The overall advantages of this approach are:

  - It is simpler to implement and requires less overhead and cost;
  - It places the onus for assessment on the TLD’s owners/operators, which could incent them to improve their compliance; and,

- It places liability on the TLD owners/operators.

The overall disadvantages include:

- It may be inadequate in providing a proper level of assurance and accountability to warrant HSTLD verification; and,
- Companies may be reluctant to publicly disclose security vulnerabilities (as an aspect of their risk management program).

The Group did discuss how the scorecard option could be enhanced with the addition of a requirement for independent third-party verification, but ultimately those discussions led the Group back into many of the key disadvantages of the “Formal Verification” option.

Interestingly, despite the perception of stronger disadvantages to the “Formal Verification” option, a straw poll of Group members taken during its deliberations indicated that 50% of those responding supported the concept that the HSTLD Program should contain a certification program option, while only 25% of those responding felt the program should contain a scorecard option. (Though 67% of that 25% also felt the scorecard option could be enhanced with an independent assessment option.)

Ultimately, despite significant discussion around this topic, the Group did not reach consensus on a particular methodology. If the decision is made to continue to move forward with the HSTLD Program, this matter will need to be resolved.

7.0 DETAILED ANALYSIS OF PUBLIC COMMENTS

The Group published two progress reports (i.e., snapshots) of its work-to-date during the course of its deliberations. A summary of those status reports are provided in Section 3.0 of this report. What follows below are summaries of the comments received on the snapshots as well as an analysis of how the Group has or has not incorporated the comments into their work. The Group has done its best to capture and present the highlights of all the submissions, and comments in their entirety may be viewed at the referenced links.

The first public comment period was open from 22 February 2010 through 8 April 2010 and the second public comment period was open from 16 June 2010 through 21 July 2010. The majority of the comments can largely be grouped into the following categories:

- The HSTLD Program should be mandatory;
- The HSTLD Program should identify classes of names that should be subject to the Program;
- New gTLD applicants who agree to participate in the Program should receive higher scoring and thus an advantage in the new gTLD process;
- The HSTLD Program should extend through the domain name registration value chain (i.e., registrars and registrants); and,
- Development of a HSTLD Program is out-of-scope for ICANN’s limited coordination role.

This section does not include public comments submitted on the various versions of the Draft Applicant Guidebook that mentioned efforts to mitigate malicious conduct including the HSTLD Program as those comments were addressed by ICANN Staff in the summaries and analyses of Draft Applicant Guidebook v3 and Draft Applicant Guidebook v4. The summary and analysis of comments on the Proposed Final Applicant Guidebook may be viewed here.

Submitter's Name **Submission Date** **Link to Comment**	**What did they say?**	**How has the AG incorporated or not incorporated the comment into its work?**
Dave Smiley, 10 March 2010 http://forum.icann.org/lists/hstld-snapshot-15feb10/msg00000.html	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. 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. 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)	The potentially voluntary nature of the HSTLD Program would allow anyone in the Internet community to decide for themselves the value of using or not using a certain TLD, and would not be subject to regulation. TLDs that wish to distinguish and differentiate themselves from others in the marketplace would have the option to demonstrate a higher level of security. Further, it is not anticipated that ICANN would benefit from any potential Program that might be implemented as any fees that might be earned from those Registry Operators seeking HSTLD verification would be earned by the assessors/evaluators that offer auditing or attestations services in support of the Program. There have been extensive discussions within the Group about how security might be extended through the domain name registration value chain from registries, to registrars, and ultimately to registrants and users. The benefits statement in Section 2.0 of this report is intended to

	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.	demonstrate how the value chain could be positively impacted by such a Program.
Steve Metalitz for the Coalition of Online Accountability, 8 April 2010, http://forum.icann.org/lists/hstld-snapshot-15feb10/msg00001.html	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? 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. Whatever approach ICANN ultimately	There are several questions in the Applicant Guidebook (e.g., #28, Abuse Prevention and Mitigation and #35, Security Policy) that require a detailed explanation of policies and procedures registries will implement to help prevent and/or expedite responses to malicious conduct. There is no single solution for solving the potential for malicious conduct and the HSTLD Program is intended to be one such mechanism that a registry could adopt that could increase the level of trust and confidence in the TLD. There is no current effort within the new gTLD Program to create classes or categories of names including those that might be subject to an increased level of malicious conduct. The approach and concept was

	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.	followed by the Group was that entities who face higher risk would identify themselves and have this voluntary Program available. At this time ICANN does not intend to introduce an objection process in the area of potential for malicious conduct. In order for such a process to be considered, clear, objective criteria must be devised. No public comment to date has suggested such criteria. Neither has discussion among the implementation team and the community resulted in a viable objection mechanism. Evaluators will be asked to ensure that security measures are commensurate with security needs. Additionally, public comments will be used to inform evaluation panels as part of their application analysis.
Claudio Di Gangi for the INTA Internet Committee, 8 April 2010, http://forum.icann.org/lists/hstld-snapshot-15feb10/msg00002.html	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. 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	The comments submitted by INTA are consistent with others that have participated in the public comment process. See above remark regarding potentially voluntary nature of the Program. The work of the Group is independent and therefore has no impact on the rights protection mechanisms that are defined in the latest version of the draft Applicant Guidebook. The work of the Group has focused on policies and procedures registries could implement in the potentially

	for some registries to cut corners. Therefore, regular, independent certification is essential to the credibility of HSTLDs. 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. 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. 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	voluntary Program. This work to date has not extended to enhanced identity verification for domain names in TLDs. Similar to comments made by the Coalition for Online Accountability, INTA suggests that classes of TLDs be identified as those who should be required to participate in higher security practices such as those defined in the draft HSTLD criteria, and that there be preference in awarding TLDs to applicants that agree to employ security levels consistent with the nature of their TLD. Defining classes of TLDs is out of scope for the group's work and such efforts have not been widely accepted in development of the new gTLD program. Several INTA comments are around auditing and verification practices that could be implementation activities for an HSTLD Program. If additional work on the Program continues, such details could be developed particularly with the assistance of firms that offer expertise in auditing and verification practices. As noted above, auditing or attestation services would be funded by fees Registry Operators would pay to independent firms that choose to offer the HSTLD designation.

	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.	
	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.	
	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).	Regarding a user-friendly and quick way to identify a domain name with the HSTLD, for example similar to the "s" in "https", the Group discussed this and agreed that a recognizable indicator of HSTLD could be important. This indicator is a level of detail that would be investigated in any ongoing HSTLD Program development work.
	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	Benefits to registrants and end users are presented in Section 2.0 of this report. Marketing and communications activities of a program are levels of implementation detail that were not considered by the Group.

	applicants that agree to be part of the HSTLD program be awarded more points in the application process.	
David Maher for the Registries Stakeholder Group, 8 April 2010, http://forum.icann.org/lists/hstld-snapshot-15feb10/msg00003.html	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. 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. 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. 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	The Group was formed to study and develop proposed solutions to establishing a high-security TLD verification program. The current vision of the Program is that it would be independently operated and that ICANN would be a participant in the ongoing development of a set of standards that could be adopted by registries wishing to participate in the Program. ICANN's role would be limited to supporting the program by facilitating an open and collaborative dialogue with the community around standards and control criteria. The ICANN Board Resolution on 25 September 2010, provided clarity to the community about ICANN's role: "ICANN will not be certifying or enforcing the HSTLD concept; ICANN is supporting the development of a reference standard for industry that others may choose to use as a certification standard of their own. ICANN will not endorse or govern the Program, and does not wish to be liable for issues arising from the use or non-use of the standard." Through the work of the Group it became clear that while there is some interest in deploying policies and procedures to mitigate malicious conduct across the domain name registration

	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? 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	value chain, how this could be accomplished is neither clearly understood nor are the costs and benefits of such a Program.

	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.	
James Bladel for Go Daddy, 9 April 2010, http://forum.icann.org/lists/hstld-snapshot-15feb10/msg00004.html	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. 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. 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	As noted above in the response to the RySG's comments, ICANN and particularly the Board have been clear about the role ICANN would play in the development of an HSTLD Program. ICANN agrees with Mr. Bladel's comment that "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." As noted above in ICANN's response to Dave Smiley, ICANN will not profit from any potential Program that might be implemented as any fees that might be earned from those registry operators seeking HSTLD verification would be earned by the assessors/evaluators that have been retained by the Registry Operator. ICANN is not looking to increase its size and scope, but rather to facilitate dialogue in the community about a program

	approach may be to specify more abstract “rules of the road” for an HSTLD and allow applicants and service providers to innovate and collaborate within this basic framework. 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.	that could be developed and implemented by a third party. The Group did not undertake a study on estimated costs of an HSTLD Program or whether such a program would be financially viable or attractive to third parties. Several Group members have suggested that their work conclude with this final report and that ICANN should, as GoDaddy suggests, provide a platform to bring together interested parties to collaborate with existing standards bodies and industry experts to develop the HSTLD framework.
George Kirikos for Leap of Faith Financial Services Inc., 20 July 2010, http://forum.icann.org/lists/hstld-program-snapshot/msg00000.html	It has become abundantly clear that ICANN does not value public input, and we will passively resist by not participating in a process that only leads to predetermined outcomes. "Participation" is not sufficient if it does not impact results.	No action required
Fabricio Vayra for Time Warner, 21 July 2010, http://forum.icann.org/lists/hstld-program-snapshot/msg00001.html	The main problem remains the voluntary nature of many of the key safeguards that ICANN has proposed. To help address concerns over malicious conduct, ICANN should, at a minimum, require the registry operators of new gTLDs to implement basic procedures to help prevent, or to expedite response to, malicious conduct involving registrations that they sponsor.	As noted above, there are several questions in the Applicant Guidebook (e.g., #28, Abuse Prevention and Mitigation and #35, Security Policy) that require a detailed explanation of policies and procedures registries will implement to help prevent and/or expedite responses to malicious conduct. The HSTLD Program is intended to be one such mechanism that a registry could adopt that could increase the level of trust and confidence in the TLD.

Steve Metalitz for the Coalition for Online Accountability, 21 July 2010, http://forum.icann.org/lists/hstld-program-snapshot/msg00002.html	“Draft framework for high security zones verification” – also seems far from implementation. Clearly progress has been made by a hard-working advisory group, which “plans to publish an actionable program for community consideration and review,” though there is no timetable set for doing so. But COA remains greatly concerned that this framework, even when made “actionable,” will contribute little or nothing to the goal of “reducing the potential for malicious conduct,” because it is completely voluntary, and no gTLD applicant is given any incentive within the application process for adopting any part of it. The first option, as COA called for in its comments eight months ago, would for the High Security Zones Verification Program to be made mandatory, 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, including but not limited to copyright piracy. The second option, also pointed out by COA last November, would be to provide incentives to adopt these enhanced protections against malicious conduct, by giving an applicant who did so extra points in the evaluation process, or taking away some points from applicants who failed to meet these standards. A third option, as described above, would be to give someone the role of objecting to any application for which, by its nature, the failure to provide enhanced protections would inappropriately expose some segment of the public to an unacceptable risk of harm. See the example of .kids, discussed in Section I-B-3 above. This is clearly in some ways a less desirable option than either of the other two, since it would delay to a later point in the process the elimination of new gTLD applications	If work on the HSTLD designation progresses, be it in its current form or possibly a reconstituted group of security and technology experts, ICANN welcomes the support of the community, including the COA, to investigate such a process. 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. 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. The new gTLD program provides for a community objection process that is detailed in Section 3.1 of Module 3 of The Proposed Final Applicant Guidebook 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.

	that carry with them excessive risk.	
Richard Tindal, 21 July 2010, http://forum.icann.org/lists/hstld-program-snapshot/msg00003.html	I am strongly of the opinion it should remain voluntary so that consumers in the marketplace have the ability to make their own assessment of the worth of the program and choose between high security TLDs and other TLDs. If there is real consumer value in the program market forces will drive its broader adoption.	No action required.
Jon Nevett, 22 July 2010, http://forum.icann.org/lists/hstld-program-snapshot/msg00004.html	I'd like to commend the work of this group in preparing a model for a high security zone TLD. I agree with the almost uniform view of the Working Group that such a program should be voluntary in nature.	No action required.

8.0 LESSONS LEARNED

In the absence of consensus about the path forward for the Group and a specific recommendation for the implementation of an HSTLD Program, what follows is a summary of lessons learned from issues the Group faced during its work. The issues are organized in the following four sections: methodology, scope, work product, and process.

Methodology:

Issue 1: The inability to correlate audit of control with measurable operational outcomes: The methodology adopted by the working group should be capable of associating cause and effect.

Issue 2: The inability to distinguish existing "community-based" and "standard" application types: The methodology adopted by the working group should be capable of distinguishing between fundamental characteristics of registries.

Issue 3: The inability to test method and model: The methodology adopted by the working group should be capable of proof of utility.

Issue 4: The inability to refer to existing security evaluations, e.g., Common Criteria ISO/IEC 15408, controlling legislation, e.g., the Federal Information Security Management Act, or programs, or implementing programs, e.g., the National Information Assurance Partnership: The methodology adopted by the working group should be informed by prior art.

Issue 5: The inability to refer to the functional specifications for, or source code of any component of a shared registry system (registry function), or any component of a shared registry system access element (registrar function): The methodology adopted by the working group should be capable of functional association with a registry service model.

Scope:

Issue 1: In scope vs. out of scope; The inability to distinguish "TLD security" from the WHOIS issue and its surrogates: The statement of scope adopted by the working group should address the distinction between “TLD security” and the WHOIS issue.

Issue 2: In scope vs. out of scope; The presumption that the HSTLD purpose extends to all existing TLDs: The statement of scope adopted by the working group should consider whether to exclude the com/net/org/biz/info market and the country code market.

Work Product:

Issue: The inability to obtain comparable RFI responses and to identify a "seal" or equivalent vendor: The RFI was written broadly to solicit information from a set of experts that weren’t directly involved in the project. Outreach to potential respondents should occur prior to the development of the RFI and outreach should be made to a broader range of respondents.

Process:

Issue 1: The process leading to the establishment of a working group: The process under which the working group conducts its work, and the process under which the working group concludes its work should be documented.

Issue 2: The effect of isolation from all other critical infrastructure protection projects: The process should have a formal relation to one or more landmark projects in the problem domain of distributed systems and information security.

9.0 RECCOMENDATION

There is consensus within the Group that more work could be done to develop an HSTLD Program, but that it must be facilitated by a community working group comprised of a multi-disciplinary team of experts. Some members of the Group that have suggested that any future effort should deconstruct the current Program model into a series of business and operational processes, and that the Program should make use of established auditing or control standards that are currently employed such as ISO27XXX. In parallel, the aforementioned community working group should consider and work with auditing and assessment standards organizations to define DNS control elements that are new, different or unfamiliar to traditional assessors. The purpose of deconstructing the work is to extract from the current Program control set those that are well known and established standards that are already served by auditing firms. Several existing gTLD registries undergo regular business and operational audits as part of their SAS 70 certification. Acknowledging that these controls are already considered in common gTLD registry audits will reduce the cost and complexity of an HSTLD Program without altering the scope of the program.

It’s been recommended that any group assembled to participate in the ongoing evolution of an HSTLD Program establish a common understanding of what is meant by a “high security TLD” and develop metrics to support that label. Some other questions to be considered for the next phase of any HSTLD work include, but are not limited to:

- What is the problem that will be solved by a Program?
- What are the intended effects of the Program and how will that be measured?
- Who will be affected by a Program and have they been involved sufficiently its development?
- Who should “champion” development of a Program?
- What are the deliverables of work in support of a Program?
- What is the problem (or puzzle) to be solved?
- What aspects of the Program are intended to assess the security of a registry?
- What aspects of the Program are intended to build trust and confidence in a registry and associated registration services?

ANNEX A – SCORECARD PROPOSAL from Michael Palage

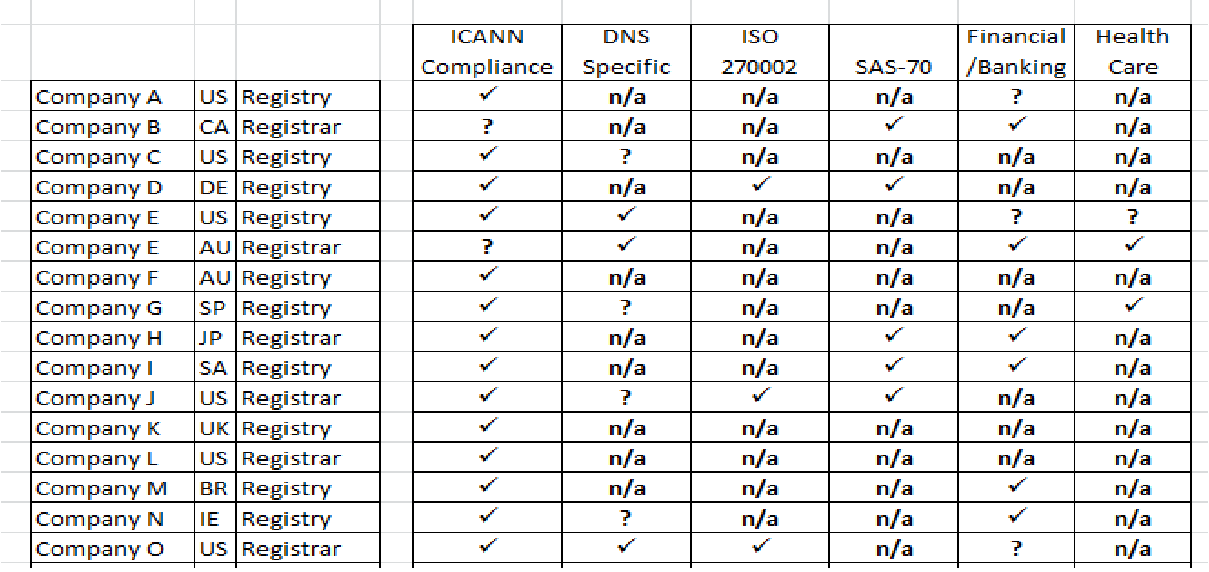
The Trust/Security Scorecard Proposal

The Scorecard proposal is designed to provide users within the domain name system a quick visual representation of relevant criteria to educate them about important security and trust criteria and to empower them to make informed decisions. The key aspects of this proposal include:

- **VOLUNTARY**: A largely voluntary approach in which registration authorities make the decision of whether or not they participate in the program. The only non-voluntary criteria being ICANN contractual compliance that will be required for all ICANN contracted parties;
- **COST SAVINGS**: Allows registration authorities that have already undergone audits and certifications in connection with other business operations to reflect these audit or certification results in the scorecard system without having to pay additional audit fees and costs;
- **INCLUSIVE**: Empowers smaller registration authorities, especially from developing countries or regions, to participate in the program without having to pay substantial audit fees and costs;
- **SCALEABLE**: Allows for the inclusion of new security/trust criteria elements ("pillars") as the market evolves with the additional of new classes of gTLDs (e.g. banking/financial, health care, city, etc.)
- **DELEGATABLE**: Allows for the delegation and maintenance of specific criteria elements ("pillars") to industry specific groups; and
- **STANDALONE**: The proposed scorecard system is intended to be a standalone program independent of ICANN's proposed new gTLD program.

The genesis of the scorecard concept lies in the detailed product/service report matrixes common in advising consumers about making an informed purchasing decision. However, after the publication of the HSTLD Snapshot #2 report which included several hundred control elements, it became clear that conveying this information in a useful and intuitive manner would be a challenge. Therefore it was decided that instead of focusing on the creation an overly comprehensive list of security trust and control elements, which would in effect be duplicating numerous other trust and security programs, it would be more prudent and efficient to leverage existing programs and figure out how to incorporate these programs into a useful framework for Internet users/consumers.

Listed below is visual presentation of a sample Scorecard Program:

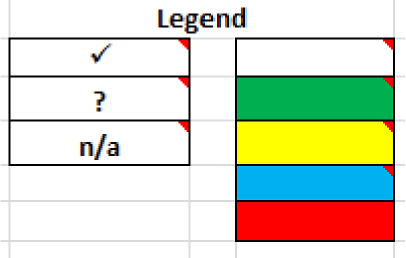


			ICANN Compliance	DNS Specific	ISO 270002	SAS-70	Financial /Banking	Health Care
Company A	US	Registry	✓	n/a	n/a	n/a	?	n/a
Company B	CA	Registrar	?	n/a	n/a	✓	✓	n/a
Company C	US	Registry	✓	?	n/a	n/a	n/a	n/a
Company D	DE	Registry	✓	n/a	✓	✓	n/a	n/a
Company E	US	Registry	✓	✓	n/a	n/a	?	?
Company E	AU	Registrar	?	✓	n/a	n/a	✓	✓
Company F	AU	Registry	✓	n/a	n/a	n/a	n/a	n/a
Company G	SP	Registry	✓	?	n/a	n/a	n/a	✓
Company H	JP	Registrar	✓	n/a	n/a	✓	✓	n/a
Company I	SA	Registry	✓	n/a	n/a	✓	✓	n/a
Company J	US	Registrar	✓	?	✓	✓	n/a	n/a
Company K	UK	Registry	✓	n/a	n/a	n/a	n/a	n/a
Company L	US	Registrar	✓	n/a	n/a	n/a	n/a	n/a
Company M	BR	Registry	✓	n/a	n/a	n/a	✓	n/a
Company N	IE	Registry	✓	?	n/a	n/a	✓	n/a
Company O	US	Registrar	✓	✓	✓	n/a	?	n/a

Along the Y axis of the Scorecard is a listing of all ICANN registration authorities (registrars/registries). The first column would include the legal name of the entity, the second column would report the national jurisdiction in which the registration authority is incorporated and/or principally operates, and the third column would indicate the specific role of the registration authority (registrar/registry).

Along the X-axis of the Scorecard is a "collapsed" view of the various pillars of trust and security criteria that registration authorities are measured against. Most of these pillars are intended to be proposed and/or designed by independent organizations which would be included into the Scorecard Program upon acceptance by ICANN. Details on the administration of how these pillars would be accepted and/or rejected from the scorecard program are provided in more detail below. The only pillars which are proposed to remain primarily within the ICANN community are ICANN compliance and DNS Specific.

The collapsed view of the scorecard can more easily be understood by reference to the following legend integrated into the scorecard:

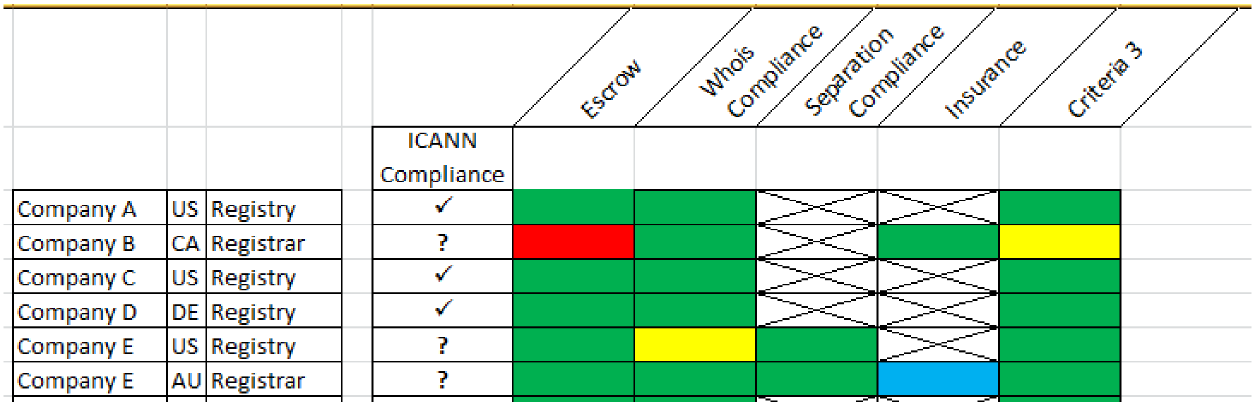


Legend	
✓	⬜
?	🟩
n/a	🟨
	🟦
	🟥

The left side of the margin illustrates the following three indicators:

- A check mark indicates that a registration authority is in full compliance with that trust/security criteria pillar;
- A question mark which indicates that the registration authority is in less than full compliance with that trust/security criteria pillar; and,
- The text N/A stands for not-available meaning that the registration authority has not provided any data to make a representation in connection with that criterion.

While the “collapsed” view of the various security/trust pillars provide a user some information to differentiate among the different registration authorities within the domain name system, by “expanding” any one of the trust/security pillars a user is given a much more detailed set of information to make an informed decision as illustrated below under the ICANN Compliance pillar:



			ICANN Compliance	Escrow	Whois Compliance	Separation Compliance	Insurance	Criteria 3
Company A	US	Registry	✓	🟩	🟩	☒	☒	🟩
Company B	CA	Registrar	?	🟥	🟩	☒	🟩	🟨
Company C	US	Registry	✓	🟩	🟩	☒	☒	🟩
Company D	DE	Registry	✓	🟩	🟩	☒	☒	🟩
Company E	US	Registry	?	🟩	🟨	🟩	☒	🟩
Company E	AU	Registrar	?	🟩	🟩	🟩	🟦	🟩

To help users more easily interpret this larger data set of criteria, the scorecard makes use of a color coded scheme as identified in the legend above.

The right side of the margin illustrates the following five color states:

- **WHITE**: The registration authority has not provided any data to participate in the scorecard program;
- **GREEN**: The registration authority has met the control criteria and it has been validated by a third party;
- **YELLOW**: The registration authority has self-validated the control criteria but has not received an independent third-party attestation;
- **BLUE**: The registration authority is in compliance with this control criteria, however, within the last twelve months that registration authority has been held in breach of that element; and
- **RED**: The registration authority is currently in breach of this control criterion.

As noted above while the scorecard is intended to be a voluntary program, the only exception to this program is the ICANN Compliance “pillar” in which all ICANN contracting parties will be scored by ICANN compliance staff. Since this pillar is mandatory, an “N/A” is not a possible option for this part of the scorecard matrix.

IMPLEMENTATION STEPS

Implementing the Trust/Security Scorecard program is rather straightforward and can leverage the existing work of the Group by taking the following steps:

- The creation of a multi-disciplinary standing committee to serve as a “trustee” of the Scorecard. It is proposed that this standing committee be called the Trust/Security Scorecard Standing Committee (TSSSC). To jump start the work of TSSSC, all Group members in support of the Scorecard proposal would be encouraged to join.
- TSSSC would begin immediate interaction with ICANN Compliance staff to propagate the initial ICANN Compliance security/trust pillar criteria and ranking.
- TSSSC would also work closely with ICANN technical staff to see about incorporating this scorecard into the existing ICANN dashboard metrics program.
- TSSSC would recommend the creation of a cross-constituency working group within the relevant ICANN community to timely develop the DNS specific control criteria. It is proposed that this working group be co-chaired by a representative from SSAC and TSSSC. While most of the DNS specific control criteria are likely to be technical in nature, the experience of the Group has demonstrated the need for a multi-disciplinary approach toward increasing trust and security to the end user.
- TSSSC would engage in outreach to increase the diversity of TSSSC membership particularly in the fields of Internet browsing and email security, as well as to raise awareness among different interest groups that might propose different trust/security pillars.
- The trust/security pillars illustrated in the mock-up are not intended to be static. In fact some of the pillars could branch out to include multiple independent sets of criteria. For example under the financial/banking pillar, it is possible for different international recognized organizations to propose different standards, e.g. BITS, World Bank, Swiss Bankers Association. The TSSSC will have to ensure that procedures are put in place to properly vet criteria/pillars before their inclusion into the Trust/Security Scorecard Program.
- TSSSC will have to discuss potential options to incorporate into the scorecard to distinguish between periodic and point-in-time audits.
- Given the independent standalone nature of the TSSSC it is proposed that any all references to the Group be removed from the Applicant Guidebook.
- TSSSC will have to develop procedures by which ICANN can approve authorized companies to conduct these audits, similar to the manner in which ICANN currently approves third parties to administer UDRP proceedings.