Introduction

ICANN's 22 September 2010 publication of the HSTLD RFI reported the purpose of the RFI is to assist the ICANN community in understanding potential frameworks and approaches to evaluate new gTLD registries against the criteria in the draft HSTLD Program, determine where improvements to draft criteria and the overall program may be necessary to ensure its success, and to assess the viability of the proposed HSTLD Program.

As the HSTLD Advisory Group (AG) noted during its 3 November 2010 call, the ICANN Board resolved on 25 September 2010 that, "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." However, while the Board said it will not be signing on to be the operator of such a product, it does support its concept just as it has other measures (e.g., URS, prohibition of wildcarding, centralized zone file access, etc.) to mitigate malicious conduct in new gTLDs. The HSTLD program or some similarly labeled standard could for example be undertaken by an outside standards organization such as the National Institute for Standards (NIST), the International Organization for Standardization (ISO), etc.

Below are the questions that responding parties submitted regarding the RFI. Suggested remarks and answers accompany the questions. Responding parties may find the MP3 recording from the 15 November 2010 HSTLD call (available at http://audio.icann.org/hstld-call-20101115-en.mp3) useful as they prepare their final response to the RFI that is due by 17 December 2010.

1. In ICANN's "Internet Corporation for Assigned Names and Numbers Request for information High Security Zone Verification Program" ("RFI"), ICANN states that "ICANN would maintain a list of approved evaluators and retain oversight and authorship of the <HSTLD> control elements." (Remark: A potential HSTLD Program is being explored by ICANN in coordination with the HSTLD Advisory Group. As noted in the RFI and published HSTLD Snapshots (see Section 2.4; Group Goal Statement), the viability of such a program is currently under review. Therefore, while the RFI includes that "ICANN would maintain a list of approved evaluators and retain oversight and authorship of the HSTLD control elements" that was the conceptual thinking when the RFI was drafted.) During the 15 November 2010 HSTLD call, ICANN executive management clarified that validation/certification is best done by a recognized standards organization that could operationalize the control elements and standards developed by the AG.)

2. How does ICANN anticipate continuing oversight and authorship of the HSTLD control elements? (Response: Working with HSTLD evaluator(s), ICANN could envision continuing some level of involvement including recommending HSTLD control elements through ongoing collaboration with the HSTLD Advisory Group or some other community-based working group that might be established to support the evolution of the control elements. If and when the control elements and standards have been incorporated to the verification process by the standards organization that develops the HSTLD program, that organization

would have oversight and authorship of the control elements.)

3. In this model, would HSTLD evaluators be able to work with ICANN and/or the community to refine the criteria as needed for audit purposes? (Response: Yes and see response to 1a.)

4. Does ICANN envision that it will "own" and "issue" a "Seal" for the TLD's that successfully demonstrate their compliance with the HSTLD control criteria? If so, how does ICANN envision preparing and hosting/managing such a seal? (Response: ICANN will not "own" or "issue" a "seal" for the TLDs that successfully demonstrate their compliance with the HSTLD control criteria. Ownership of a seal would belong to the standards organization of competence in this area that is responsible for its development. Issuance of a seal would likely belong to the assessors or evaluators that implement the program. It may be that the third-party or parties that implement the HSTLD program would "own" or "issue" a "seal" and ICANN might list them on www.icann.org as approved HSTLD providers. Listing the third-party HSTLD providers on ICANN's website could be seen as a way to legitimize the program.)

5. According to section 2 of the RFI, "An ICANN generic TLD registry operator is contractually obliged to provide all ICANN accredited registrars with equal access to the ability to process domain name registrations for labels assigned from its TLD. This results in a fan-out from registry operator to registrar on the order of 100s of accredited registrars." Under this model, is it possible for a TLD registry operator to require that all registrars seeking to process domain name registrations in the registry operator's TLD comply with the requirements of the HSTLD criteria? (Response: It is possible under this model for a TLD registry operator to require its registrars comply with the requirements of the HSLTD criteria. All registrars would have equal access to the ability to process domain name registrations for labels assigned from the TLD. However, it is unknown whether accredited registrars would pursue accreditation in a particular TLD with the knowledge that the registration standards for that TLD must comply with HSTLD criteria.)

6. Would a registry operator also be able to specify a sub-group of HSTLD control requirements that all registrars would be required to comply with? (Response: In certain circumstances, this may be possible, but the sub-groups would have to be defined in such a manner as to not jeopardize the purpose of the HSTLD program. In its current draft form, the concept for an HSTLD program is comprised of a set of predetermined and auditable control standards and compliance with all elements would be required to earn the HSTLD designation. Some in the community have suggested that there should be tiers of verification, but the concept of verification tiers remains an open issue. If a tiered system was to be developed, it's possible a registry-operator would be able to specify a sub-group of HSTLD requirements necessary to achieve verification for varying tiers.)

7. As stated in ICANN's RFI, section 3.1.1 of Model for a HSTLD Program identifies the program elements, objectives and sample criteria for the assessment of registrars, as a component of the HSTLD program requirements. Does ICANN envision that HSTLD assessors would complete all assessment work with HSTLD registry operators, and would gather supporting registrar control evidence from the HSTLD registry operators, or does ICANN envision that HSTLD assessors would examine registrar evidence directly? (Response: ICANN envisions that HSTLD assessors would perform all assessment work with HSTLD registry operators, and that the assessors would gather supporting registrar

control evidence from the HSTLD registry operators. Obligations for registrars could be passed down through the Registry-Registrar Agreement between the registry operator and its registrars, and similarly from registrars to registrants through the domain name Registration Agreement.)

8. What is the estimated timeline for HSTLD verification to become an actionable program? (Response: The estimated timeline for the HSTLD verification to be an actionable program is undetermined at this time. However, ICANN and its community should look to the time taken by standards organizations (e.g., NIST, ISO, etc.) that develop and implement standards.)

9. What is the planned extent of ICANN's participation in the program? (Response: ICANN will continue to participate in the HSTLD Advisory Group through the publication of their final report and recommendation. The planned extent of ICANN's participation in the program after the AG's final report will be determined after the conclusion of the RFI process. As noted above in the introduction, ICANN will continue to support the development and adoption of a reference standard for registry security that others may use as a certification standard of their own.)

10. The questions asked in the RFI can be answered in various degrees of depth. To answer them in a thorough and detailed manner, it will take considerable effort. What are ICANN's expectations with regards to the level of detail RFI respondents should be providing in their responses? (Response: ICANN appreciates the feedback it's received from respondents who have expressed a concern regarding the level of effort required to answer the questions in a thorough and detailed manner. ICANN would like to receive as much meta-level or detailed information as possible. In that regard, ICANN also understands that determining how much effort to expend on the answers is a business decision that each respondent must make and appreciates the contributions respondents make.)

11. What are the next steps, if any, for respondents of the RFI? Would non-respondents be allowed to become "approved" third party evaluators? Would the number of respondents to the RFI (e.g., you only have two respondents) influence ICANN's response to this question? (Response: ICANN may have follow-up questions to respondents' answers and would be in communication with them to ensure that information was understood as it was intended. The number of respondents to the RFI does not have a role in determining the number of potential third-party providers and therefore would not influence ICANN's response to the prior question.)

12. How does ICANN define 'Independence' as it relates to the proposed HSTLD? Has ICANN considered including independence enforcement procedures to support this requirement? (Response: Independence for the purpose of implementing a proposed HSTLD program means an entity that is owned, operated, and controlled by an entity other than ICANN or its contractual partners. However, it is envisioned that the ICANN community would continue to be involved in the process for recommending new control mechanisms that might be developed as the HSTLD program evolves over time. Since ICANN will not administer the HSTLD program, it has not considered including independence enforcement procedures to support this requirement. However, ICANN is open to hearing more from respondents about their thinking on this particular element.)

13. Is there an expectation that the HSTLD program will align with other current standards such as ISO/PCI/Other? (Response: The HSTLD program is a new concept. Certain of the

program elements have origins in other, current standards. If aligning the program with other current standards is viable, promises to reduce program overlap or complexity, or enhances the value and integrity of the program, ICANN would be open to considering such alignment. ICANN welcomes input from respondents about control mechanisms or standards that could be developed that are in alignment with other current standards.)

14. Was there consideration to using a specific country's existing attestation/compliance standards? (Response: This direction was not considered. The HSTLD Advisory Group is comprised of an international group of technical/operational/security/policy experts that could have contributed standards from a broad range of countries. Registry operations also have a global footprint. Individual gTLD registries and back-end providers operate in multiple locations worldwide, as do registrars. Certain "country code" TLD registries may also be interested in participating in the voluntary program. With this environment, primary consideration of international standards seemed prudent.)

15. Would there be a negative perception if a US based standard (AICPA) defines the methodology to deliver an opinion level service? Or, is an ICANN developed standard the only acceptable approach for the internet community? (Response: It is not possible to determine if there would be a negative perception if a US based standard defines the methodology to deliver an opinion level service. The standards in their current form are the result of a community-led, bottom-up, collaborative effort – not an ICANN developed standard unless ICANN is intended to include its community including for example the HSTLD Advisory Group. ICANN envisions that its community would continue to be involved in the process for considering new control mechanisms (i.e., standards) as the HSTLD program evolves over time.)

16. How will the empirical and opinion information gathered in the RFI process be processed into summarized results? (Response: The purpose of the RFI is to assist the ICANN community in understanding potential frameworks and approaches to evaluate new gTLD registries against the criteria in the draft HSTLD Program, determine where improvements to draft criteria and the overall program may be necessary to ensure its success, and to assess the viability of the proposed HSTLD Program. Information gathered in the RFI process will be incorporated into the Advisory Group's final report.)

17. When and how will the RFI results be distributed to the ICANN community? What impact, if any will this have on the new gTLD process? (Response: It is anticipated that the RFI results will be posted to the HSTLD information page at http://www.icann.org/en/topics/new-gtlds/hstld-program-en.htm as soon as practicable after the 17 December 2010 deadline. Given the HSTLD program is intended to be voluntary and operated by an independent third-party, the development of the concept does not impact the launch of the new gTLD application process. As noted in the Proposed Final New gTLD Applicant Guidebook published on 12 November 2010, question 35 has been amended to include information regarding augmented security levels or capabilities as a direct result of the work done in the HSTLD AG.)

18. Given recent comments made by the ICANN Board of Directors as discussed on the AG call on the October 13th, please clarify ICANN's continuing association with HSTLD and the associated zone verification program. Is the HSTLD program expected to continue absent support or involvement from ICANN? (Response: ICANN will continue to support the development and adoption of a reference standard for registry security that others may use

as a certification standard of their own. The HSTLD program or some similarly labeled standard could for example be undertaken by an outside standards organization such as NIST, ISO, etc.)

19. Is it ICANN's plan to have the HSTLD and verification program covered in the final gTLD draft applicant guidebook (DAG)? (Response: As outlined in the RFI and other publicly available HSTLD materials, the proposed program is intended to be voluntary and would be operated by an independent third-party provider or providers. Similarly to the centralized zone file access service provider program, the HSTLD program may be included in the final Applicant Guidebook as a reference. However, operational details of an HSTLD program are outside the scope of the Applicant Guidebook.)

20. What are the views and position of ICANN and the AG on making HSTLD a mandatory compliance program for new gTLDs and all or selected existing TLDs? (Response: The AG has recommended that the HSTLD verification program be voluntary and should be administered by an independent third-party provider or providers. In its voluntary form, the market will decide whether mandatory is relevant; for example, markets may force or provide incentives for TLDs to be HSTLD. Currently, there is no view or position on a mandatory compliance program for new gTLDs and all or selected existing TLDs.)

21. Has ICANN or the AG surveyed current registry operators in controlled survey format to gauge their interest in voluntarily complying with the program? Can any additional guidance be provided on the anticipated number of entities that will desire (or be required) to be verified under this program? (Response: ICANN or the AG has not surveyed current registry operators to gauge their interest in voluntarily complying with the program. At this time, it's not possible for ICANN to provide guidance on the number of new gTLD applicants or the number of entities that will desire to be verified under the program.)

22. Has ICANN or the AG considered the process to be followed if a deficiency or breach in security at an accredited participant comes to light? This may occur as part of a periodic audit, through external complaints, or self disclosure? Would you like feedback on how these events might be evaluated and the actions that ICANN might take in response? (Response: No we haven't considered this at this time, but we recognize that the legitimacy of the HSTLD program rests not only in its definition but execution, and that a compliance program with appropriate enforcement mechanisms and remedies must be developed. ICANN and the AG welcome all feedback on any proposed process for the program.)

23. Is it the intent of the HSTLD zone verification program to provide a full top-down assurance model, i.e. registrars and registries? In other words, provide assurance about the entire value chain? Or, is the intent to provide a selective assurance model regarding only those entities that elect to participate, regardless of the other entities in the value chain they interact with? (Response: Yes, the intent of the HSTLD program is to provide an increased level of assurance about the entire value chain. It is for this specific reason that draft control elements have been proposed for registries, registrars and registrants. Further, just as registries could impose requirements on registrars through the Registry-Registry Agreement, registries could impose requirements on registrants (e.g., registries could require membership in a specific kind of association.))

24. Regarding the verification of registrars, is their participation in the verification program contingent on (1) the registrar being accredited with ICANN, and/or (2) the registries it works

with having successfully met and been verified against the HSTLD requirements? (Response: The HSTLD program is intended to verify registry operators. However, registrars that would elect to distribute domain names in an HSTLD verified TLD would be subject to program requirements that the registry operator would likely pass through to them via the Registry-Registrar Agreement between them. In the case of gTLD registry operators that pursue HSTLD verification, their registrars must be ICANN-accredited as only accredited registrars may sell domain names in gTLD registries.)

25. What level of review are ICANN and the AG expecting in the response to question 8 and 9 concerning the accuracy and completeness of the HSTLD Control Worksheet? Is ICANN and the AG looking for systemic issues with the worksheet or a thorough review and critique? (Response: ICANN and the AG appreciate the level of effort it would take to provide a thorough review and critique of the control elements as queried in questions 8 and 9. Therefore, we defer to your judgment about the appropriate level of effort given the time and considerable breadth of the questions.)

26. We believe it would be helpful to have an in-person meeting following the submission of the RFI to discuss our responses and possible strategies for the HSTLD program. Would ICANN and/or the AG be willing to host such a session to discuss our RFI responses in more detail? (Response: ICANN and/or the AG would be willing to consider subsequent communication after the receipt of the RFI response and after the close of the RFI submission period.)

27. Does the HSTLD program aim to commoditize the most complex and critical aspects of running a secure registry operation? (Response: No, the program is voluntary, and attempts to identify that if a particular TLD faces an exceptionally high risk of malicious conduct, applicants should be required to demonstrate a commensurate commitment to the provision of strong security policies and procedures. Satisfying the control criteria will not create a secure registration that is interchangeable across HSTLDs. Rather, the program is intended to provide increased confidence for registrants and users that a TLD meets certain security criteria that the registrants and users perceive as necessary for the operation of a registry, whether that registry serves a community, industry, vertical market, financial sector, etc.).

28. How will HSTLD verification measure real-world experience and the extent of global relationships needed to diagnose and neutralize a security threat? (Response: Real world experience in managing security threats is quantifiable in terms (i) the number of staff-years of experience an organization employs to manage security threats, (ii) demonstrations of competency in security threat management such as security certifications, and (iii) continuing education provided by an organization for staff and management responsible for security threat management. For example, in order to pass the audit criteria (i.e., Section 2.1.5. use of WebTrust EV 25.2 addresses registry operator personnel training) the applicant seeking HSTLD verification would have to describe how confidence in staff translates into satisfying the criteria.)

29. Will HSTLD verification attempt to measure a TLD's adaptive responsiveness or will operators be re-verified whenever new threats or vulnerabilities are discovered? (Response: This is a challenging area to measure. However, the issue is one that is problematic for Internet infrastructure, critical infrastructure, enterprise, and generally, any organization where Internet presence is mission or business critical. In the absence of methods to quantify and assess “adaptive responsiveness”, however, it is possible for an assessment to determine that a TLD is as well prepared to adapt to an evolving threat landscape as best

practices, experience, and technology provide. Re-verification may be warranted similarly to industry practices used to validate compliance with other security standards such as ISO 27001.)

30. How will ICANN's HSTLD program verify and/or measure relevant security experience and performance in the face of evolving security threats and vulnerabilities? (Response: As indicated in the criteria developed by the AG, the program must assess the competencies of the security team of an organization. There's no point in insisting on security practices for hardware, software, and network configuration if staff is not capable of implementing and maintaining the control criteria. However, assessing staff is more measurable today than it was 10 years ago because of the (obvious) 10 years of cumulative experience organizations have accumulated by dealing with a growing presence/threat of attacks, the rise of numerous security certifications that focus on forensics, countermeasures, and incident response, and the establishment of best practices and standards for security at management and staff levels.

    Experience can be measured in terms of the number of staff-years an organization can apply to risk assessment, threat mitigation, detection and response. Skill and knowledge base is measured in formal training, certification, and continuing education of the security staff. Using these (and probably other) metrics, the program can establish an industry baseline for the caliber and number of security staff an organization will need to provide high security. For example, for a given organization, it is possible to determine whether the security competencies meet or exceed the competencies of other organizations with similar risk/threat profiles.)