24 NOVEMBER 2009

Briefing Paper - Advisory Group approach to discussion (benefits and methods) to effectively and efficiently enhance access to zone file information (anticipating an environment with many gTLDs).

Issue: Individuals or entities ("interested parties") seek zone file information for legitimate purposes including anti-abuse efforts, law enforcement activities, academic research, and intellectual property protection. Currently, interested parties must contract with each gTLD registry operator to obtain access to zone data. To support access, each gTLD registry operators allocates resources to administer and distribute its zone file to interested parties who agree to abide by the registry's terms of service per an appendix to their Registry Agreement.

The ICANN process to expand the namespace to tens or perhaps hundreds of new gTLD could result in scaling challenges for interested parties to continue to collect and compile gTLD zone files for legitimate purposes. gTLD registry operators would continue to bear the costs of administering their zone file access provisions.

Questions: Describe the benefits of providing or need to provide efficient access to zone file data. What solutions are available to the community to increase the efficiency of zone file distribution for gTLD registries and interested parties and to safeguard the interests of all parties, including gTLD registries?

Process: ICANN will convene an advisory group to include gTLD registries and interested parties to produce a requirements statement considering both the vendors and consumers of gTLD zone data; and then identify how enhancements could be made to the current system for accessing gTLD zone files.

Elements to be considered:

1. What members of the community should be invited to participate in the advisory group?
2. What are the issues the advisory group should address?
3. What are potential solutions to the issues?
4. What are the legitimate uses of zone file access and who should have it?
5. What are the advantages of a centralized approach to zone file access as a potential solution?
6. What are the disadvantages of a centralized approach to access?
7. Registry operators currently vet users and monitor access to zone file data by responsible parties for legitimate purposes; could a centralized approach maintain such safeguards?
8. Can a centralized approach offer a more secure, stable and resilient alternative to the current approach?
9. What are the concerns to be considered if a centralized approach to access is established? For gTLD registry operators? For interested parties?

Briefing Paper - Advisory Group approach to discussion (benefits and methods) to enhance trust within appropriately verified TLDs.

Issue: The High Security Top Level Domain Verification Program ("HSTLD") or ("Program") is designed to provide a structured approach to improve Internet community trust and to improve the overall security of the domains registered within Top Level Domains ("TLD") that volunteer to participate in the Program. The Program draft (see additional information below) currently provides a framework that describes a voluntary Program for Registries that elect to self-identify as a "high-security" TLD. By electing to be identified as a "high-security" TLD, the Registry is signaling its intent to meet the requirements of the HSTLD Program. This Program has been developed based on comments received from ICANN stakeholders that were gathered during the feedback process for the establishment of new TLDs, as well as examination of other certification-type programs. The Program incorporates input from internationally recognized control and certification standards such as the AICPA/CICA Trust Services and the ISO/IEC 27000 series.

Benefits: The Program allows for an enhanced level of trust for the Internet users within a HSTLD. Trust is established by allowing the HSTLD Internet users to see, through an appropriate seal, that the TLD has achieved Security Verification. By achieving the seal, the TLD operator will have demonstrated that it has implemented the required control environment defined by the Program, and that the required controls were operating effectively during a period of review. The Program will require the Registry to both implement controls and to undergo a periodic audit per the requirements of the Program. The balance between benefit (enhanced trust) and cost constitutes the key business decision that a TLD operator will use as the basis to determine if the Program is an appropriate business process to pursue.

Process: ICANN will convene an advisory group to include TLD registries and interested parties to produce a requirements statement considering both the vendors and consumers of a TLD verification program; and then identify how an HSTLD program could be implemented and managed.

Elements to be considered:

1. What members of the community should be invited to participate in the advisory group?
2. Are there existing certification programs in one or more industries that can serve as a model for the HSTLD program?
3. What are the costs/benefits to ICANN of development of the Program, i.e., how many TLDs might opt to pursue a verification seal?
4. What are the issues the advisory group should address? Some initial issues raised include:
    a. Incentives – Potential incentives (beyond market value) should be considered as a component of the program.

b. Background Checking – The ability for an assessor to obtain valid background checks in a global implementation will need to be examined.

c. Assessor Requirements – Full requirements to become a Security Verification Program Assessor will need to be developed and published. Requirements will also need to define assessor independence.

d. Metrics and Reporting – Development of standardized metrics and report templates designed to report compliance to the governance body, management team, the Board, and the Internet Community. These reports and metrics would be published.

e. Limitation of Liability – Key issues and resolutions around issues of liability related to the program will need to be identified and resolved.

f. Anticipated Fees - At this stage in development, fee structure for the program has not been decided. It is anticipated that Registries wishing to pursue Security Verification will be required to pay fees for the evaluation of operation of controls in their environment.

5. What are potential solutions to the issues?

Additional Information: For additional information, please refer to the following sources:

Source	Link	Last Update
High Security Top Level Domain Verification Program Concept Paper[1]	**http://www.icann.org/en/topics/new-gtlds/high-security-zone-verification-04oct09-en.pdf**	Oct 2009

[1] NOTE: The concept paper was originally called the "Voluntary Security Designation" program. The name of the program has changed to the "High Security Top Level Domain Verification" program as the concept is now becoming a working program.