New gTLD Program
Explanatory Memorandum

Mitigating Malicious Conduct

Date of Publication: 12 November 2010

Background – New gTLD Program

ICANN was founded ten years ago as a not-for-profit, multi-stakeholder organization dedicated to coordinating the Internet's addressing system, one of its foundational principles, recognized by the United States and other governments, has been to promote competition in the domain-name marketplace while ensuring Internet security and stability. The expansion of the generic top-level domains (gTLDs) is a platform to allow for more innovation, choice and change to the Internet's addressing system.

The decision to introduce new gTLDs followed a detailed and lengthy consultation process with all constituencies of the global Internet community represented by a wide variety of stakeholders – governments, individuals, civil society, business and intellectual property constituencies, and the technology community. Also contributing were ICANN's Governmental Advisory Committee (GAC), At-Large Advisory Committee (ALAC), Country Code Names Supporting Organization (ccNSO), and Security and Stability Advisory Committee (SSAC). The consultation process resulted in a policy on the introduction of new gTLDs completed by the Generic Names Supporting Organization (GNSO) in 2007, and adopted by ICANN's Board in June, 2008.

This explanatory memorandum is part of a series of documents published by ICANN to help the global Internet community in understanding the requirements and processes presented in the Applicant Guidebook. Since late 2008, ICANN staff has been sharing the program development progress with the Internet community through a series of public comment fora on the Applicant Guidebook drafts and supporting documents. All comments received are carefully evaluated and used to further refine the program.

Please note that this document is a discussion draft only. Potential applicants should not rely on any of the proposed details of the new gTLD program as the program remains subject to further consultation and revision consultation and revision.

Summary of Key Points in this Paper

- Even though nine malicious conduct mitigation recommendations have already been incorporated into the Guidebook, work on the actual implementation is ongoing.
- The solutions that have been detailed in these memoranda will result in significant improvements to the DNS environment by increasing protections for registrants, ensuring a more secure environment, and developing and implementing tools to detect and combat potential malicious behavior.

Summary

ICANN has previously published two versions of this Explanatory Memorandum intended to describe nine improvements in the Applicant Guidebook to address potential malicious conduct in new gTLDs. The first memo was published on 3 October 2009 and the second memo on 31 May 2010.

This update is intended to describe additional implementation work that has occurred in these areas – even though the recommendations have already been incorporated into the Guidebook, work on the actual implementation is ongoing.

The solutions that have been detailed in these memoranda will result in significant improvements to the DNS environment by increasing protections for registrants, ensuring a more secure environment, and developing and implementing tools to detect and combat potential malicious behavior. ICANN and the community will continue to collaborate on measures and initiatives that will contribute to the stable launch of the new gTLD process. Security, stability and resiliency issues will remain a high priority concern for ICANN as the new gTLD program evolves and proceeds towards launch and implementation.

This paper highlights the significant amount of excellent work that has been done, mostly by community volunteers in comment fora or in working groups. ICANN appreciates and is grateful for the commitment by volunteers for their work on initiatives that will significantly improve the DNS environment.

The nine recommendations that were proposed for implementation in new gTLDs that are now included or referenced in the Proposed Final Applicant Guidebook include:

1. ***Vetted registry operators*** – This recommendation requires that new gTLD applicant registry operators be appropriately reviewed, to determine if the applicant registry operator has a criminal or malicious history.
2. ***Demonstrated plan for DNSSEC deployment*** **–** This recommendation requires it be mandatory for a new gTLD applicant demonstrate a plan for DNSSEC deployment, in order to reduce the risk of spoofed DNS records.
3. ***Prohibition of wildcarding*** – This recommendation requires appropriate controls around DNS wildcarding would reduce the risk of DNS redirection to a malicious site.
4. ***Removal of orphan glue records*** – This recommendation requires that gTLDs remove name server records, when a system is removed from the gTLD, in order to reduce the risk of use of these remnant records by a malicious actor.
5. ***Requirement for thick WHOIS records*** – This recommendation requires that new gTLDs maintain and provide access to “thick WHOIS” records, to improve the accuracy and completeness of WHOIS data. The use of thick WHOIS records provides a key mechanism to combat malicious use of the new gTLDs, by providing a more complete chain of contracts within the TLD. This in turn should allow for more rapid data search and resolution to malicious conduct activities, as they are identified.
6. ***Centralization of zone-file access*** – This recommendation requires that access credentials to obtain registry zone file data be made available through a centralized source, allowing for more accurate and rapid identification of key points of contact within each TLD. This reduces the time necessary to take corrective action within TLDs experiencing malicious activity.
7. ***Documented registry level abuse contacts and procedures*** **–** This recommendation requires that gTLDs establish a single point of contact responsible for the handling of abuse complaints and that registries provide a description of their policies designed to combat abuse. These requirements are considered fundamental steps in allowing successful efforts to combat malicious conduct within the new gTLDs.

8. ***Participation in an expedited registry security request process*** – This recommendation provides that new gTLDs be enabled to take quick, effective actions in light of systemic threats to the DNS by establishing a dedicated process to review and approved expedited security requests.
9. ***Draft framework for high security zone verification*** – This recommendation suggested the creation of a voluntary program designed to designate TLDs wishing to establish and prove an enhanced level of security and trust. The overall goal of the program is to provide a mechanism for TLDs that desire to distinguish themselves as secure and trusted, for TLD business models that would benefit from this distinction.

The remainder of this memorandum will address the specific status of work regarding each recommendation.

Status of Nine Malicious Conduct Recommendations

This section provides current status of the nine recommendations designed to reduce the potential for malicious conduct in new gTLDs.

1 Vetted Registry Operators

- **Current Status**

The recommendation to require "vetting" or background checks of registry operators is a guiding principle in enhancing the application process for new gTLD applicants. The new gTLD application process contains specific criteria against which new gTLD applicants are checked as a component of the application process. The Proposed Final Applicant Guidebook has been amended to add detail and specificity in response to comment. The specific reference to terrorism is removed (as is the over-simplified list of background check areas). Background screening will be conducted in only two areas: general business diligence and criminal history; and, history of cybersquatting behavior.

2 Require DNSSEC deployment

- **Current Status**

A plan for DNSSEC deployment is a mandatory component of the new gTLD application process and a component of pre-delegation testing for each new gTLD. Specification 6 to the Registry Agreement contains a provision that: "Registry Operator shall sign its TLD zone files implementing Domain Name System Security Extensions ("DNSSEC")". Since the root zone was signed for DNSSEC on 15 July 2010, 64 TLDs (as of 11 November 2010) have signed their zones.

3 Prohibition on Wild Carding

- **Current Status**

The language related to the prohibition of DNS wildcards remains part of Specification 6 to the Registry Agreement. There has been no change in this prohibition since the ICANN Board of Director resolved at its public meeting in Sydney in June 2009 that new top-level domains must not use DNS redirection and synthesizing DNS responses.

4 Orphan Glue records

- **Current Status**

SSAC formed a working group to study this issue and a considerable amount of analysis of TLD zones and registrations has been done to obtain a clearer picture of how prevalent orphans are in major TLDs. The working group has examined zone files for all current gTLDs and has analyzed how often orphans are used for malicious conduct. SSAC has developed a draft working group report that is currently under final review by the group. The recommendations generated by the SSAC working group may offer additional guidance to registries regarding how to manage orphan records and will be evaluated for their inclusion in key gTLD processes. As noted in ICANN Board Resolution 2.8 on 25 September 2010, "Current provisions in the guidebook require each applicant to describe proposed measures for management and removal of orphan glue records for names removed from the zone. This requirement should remain in place, and will be adjusted if SSAC makes a new recommendation in its report on this issue."

5 Requirement for Thick WHOIS

- ### Current Status

The status of this recommendation is unchanged and "thick WHOIS" is a requirement for all new gTLDs. All new gTLDs will have to implement thick WHOIS requirements, per Specification 4 of the Registry Agreement. More information about this recommendation is available in the Explanatory Memorandum on WHOIS published on 30 May 2010.

Additionally, the evaluation and scoring system in the Proposed Final Applicant Guidebook has been amended to tentatively include an additional point possible for applicants who specify that they will provide a searchable Whois feature will receive an additional point.

6 Centralization of zone-file access

- ### Current Status

The recommendation to create a mechanism to support the centralization of access to zone-file records was accepted by ICANN, and an Advisory Group called the "Zone File Access Advisory Group" ("ZFA AG") was created, with the mandate to work with the community, to develop a proposal for a mechanism to support the centralization of access to zone files. The ZFA AG completed its work and details are available in its Strategy Proposal published on 13 May 2010.

In summary, the ZFA AG recommended a Hybrid Model (the "Model") that is a combination of the enhanced bi-lateral and clearinghouse models described in its proposal. The Model offers a single point of contact for applicants seeking zone file access and largely preserves existing roles and operational functions of data providers. The Model introduces two changes to the current zone file access system. First, it standardizes the relationships between zone file data providers (i.e., registry operators) and consumers (e.g., anti-abuse and trademark protection organizations, researchers, academia, etc.) in three main categories: application standards, access standards, and file/record format standards. Second, it introduces a lightweight clearinghouse for identity management in the zone file access system that is intended to provide a single point of contact for consumers who seek zone file access.

ICANN is developing a plan to identify an appropriate service provider to implement the recommendation outlined in the proposal.

References to Zone File Access can be found in Section 2 of Specification 4 to the Registry Agreement.

7 Documented Registry Level Abuse Contact and Policies

- ### Current Status

The recommendation to require new gTLDs to document a specific Registry abuse contact and to provide a description of their specific anti-abuse policies is a requirement for all new gTLDs. This has not changed since the original malicious conduct memorandum and the provision may be found in Section 5.4.1 of Module 5.

8 Participation in an Expedited Registry Security Request (ERSR) Process

- ### Current Status and/or Updates

On 1 October 2009, ICANN announced the availability of the Expedited Registry Security Request (ERSR) Process. This process is to be employed by gTLD registries exclusively for incidents that require immediate action by the registry in order to avoid deleterious effects to DNS stability or security.

The ERSR, a web-based submission procedure, represents the result of a collaborative effort between ICANN and gTLD registries to develop a process for quick action in cases where gTLD registries:

- inform ICANN of a present or imminent security incident to their TLD and/or the DNS; and,
- request a contractual waiver for actions they might take or have taken to mitigate or eliminate the incident.

A contractual waiver is an exemption from compliance with a specific provision in a registry agreement for the time period necessary to respond to the Incident.

9 Framework for a High Security Zone Verification

- ### Current Status

The recommendation to create a draft framework for high security zone verification was made by banking and financial services groups such as BITS (a consortium of financial service institutions in the US), and an initiative called the High Security Zone Top Level Domain Program ("HSTLD Program") was created. The initiative is to draft a framework of proposed controls for high security zone verification. To analyze possible approaches to such a framework and moving towards a proposal for community review ICANN formed the High Security Zone Top Level Domain Advisory Group ("HSTLD AG"). The HSTLD AG's mandate has been to work with the community, through a bottom-up development model, to propose an approach(es) to a voluntary program consisting of control standards and incentives to increase security and trust in TLDs that elect to participate in such a program. A HSTLD program would not be operated by ICANN, but rather by an independent third-party entity that would establish criteria and certify TLDs according to those criteria.

On 16 June 2010, the ICANN posted the HSTLD AG's HSTLD Snapshot #2 for public comment. The Snapshot presents a common framework of principles, criteria, and control standards that would allow TLD registry operators that are interested in achieving designation as a High Security Top Level Domain to uphold and demonstrate enhanced security-minded practices and policies. The current framework forms the basis for the core requirements of the HSTLD Program, and can be referenced in Appendix A to the Snapshot.

The public comment period on the Snapshot concluded on 21 July 2010, and the summary and analyze the comments will be been published along with the Proposed Final Applicant Guidebook. Additionally, ICANN and the HSTLD AG agreed there is value in conducting a Request for Information (RFI) on the program. The purpose of the RFI is to assist the ICANN community in understanding potential frameworks and approaches for evaluating TLD registries against the HSTLD criteria, 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.

ICANN announced the publication of the RFI on 22 September 2010 and responses are due by 23 November 2010.

After the RFI period closes on 23 November 2010 and ICANN and the HSTLD AG have had adequate time to respond to questions and to summarize and analyze the responses, a determination about next steps will be made.

ICANN remains committed to mitigating malicious conduct in new gTLDs and supports the development of the HSTLD concept as a voluntary, independently operated program.