New gTLD Program
Update to Explanatory Memorandum
Mitigating Malicious Conduct

Background - New gTLD Program

Since 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) will allow for more innovation, choice and change to the Internet's addressing system, now represented by 21 gTLDs.

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. The program is expected to launch in calendar year 2010.

This explanatory memorandum is part of a series of documents published by ICANN to assist the global Internet community in understanding the requirements and processes presented in the Applicant Guidebook, currently in draft form. 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. To date, there have been over 250 consultation days on critical program materials. The comments received continue to be carefully evaluated and used to further refine the program and inform development of the final version of the Applicant Guidebook.

For current information, timelines and activities related to the New gTLD Program please go to

http://www.icann.org/en/tlds/select.htm

Please note that this 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.

Summary

Significant progress has been made in addressing community concerns regarding mitigation of the potential for increased malicious conduct as related to the new gTLD program.

The solutions describe here will result in significant improvements to the DNS environment: providing protections for registrants, a more stable environment and tools to detect and combat potential malicious behavior. While continual improvement is always required in this area, these improvements will contribute to the stable launch of the new gTLD process. Addressing evolving security, stability and resiliency issues will remain a continuing, high priority concern for ICANN as the new gTLD program proceeds towards launch and eventual implementation and beyond.

There is a significant amount of excellent work done here, mostly by community volunteers in comment fora or in working groups. They are to be commended for significantly improving the DNS environment. ICANN tanks you.

This paper is an update to the original "Mitigating Malicious Conduct" ("malicious conduct memo") memorandum published 3 October 2009. The original memorandum is available at the following link:

http://www.icann.org/en/topics/new-gtlds/mitigating-malicious-conduct-04oct09-en.pdf

In the original malicious conduct memo, ICANN sought comments on the proposal to add specific measures to the new gTLD registry agreement, to be required of all registries in order to reduce the potential for malicious conduct within the new gTLDs.

To facilitate this process, ICANN completed a study of malicious conduct, as it related to conduct within the TLD space. During the study, ICANN staff solicited and received comments from multiple outside sources, including Intellectual Property Constituency (IPC), Registry Internet Safety Group (RISG), the Security and Stability Advisory Committee (SSAC), Computer Emergency Response Teams (CERTs) and members of the banking/financial, and Internet security communities. These parties described several potential malicious conduct issues and encouraged ICANN to consider ways these might be addressed or mitigated within the new gTLD registry agreements, or as a component of the application process. These recommended measures were intended to increase benefits to overall security and stability for registrants and trust by all users of these new gTLD zones.

The outcome of this study, and the corresponding public comment period, created nine recommendations, designed to provide areas of focus, from which controls that would reduce the potential for malicious conduct within gTLDs could be created. The nine recommendations will be implemented in the program:

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 "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 and/or updates (if applicable) to the nine recommendations designed to reduce the potential for malicious conduct in new gTLDs, as presented in the original malicious conduct memo (see "Summary of Key Points in the Paper" above). Each recommendation is broken into a "current status and/or updates" section, detailing significant updates against the recommendation, and "specific recommended improvements for the new gTLD Process" as a reference to the material published in the 3 October 2009 malicious conduct memorandum.

1 Vetted Registry Operators

- ### Current Status and/or Updates

  The recommendation to require "vetting" or back ground checks of registry operators has been a guiding principle in enhancing the application process for new gTLD applicants. The new gTLD application process now contains specific criteria requiring a new gTLD applicant to submit to various background checks as a component of the application process. In addition, as mentioned in the original malicious conduct memo, Module 2 of the Draft Application Guidebook contains specific language to the right to deny otherwise qualified applicants, should they fail a specified vetting process. The details of the criteria and language in Module 2 of the Draft Applicant Guidebook can be referenced below or in the following link:

  http://www.icann.org/en/topics/new-gtlds/draft-evaluation-criteria-30may09-en.pdf

2 Require DNSSEC deployment

- ### Current Status and/or Updates

  Evidence of a plan for DNSSEC deployment continues to be a mandatory component of the new gTLD application process and a component of pre-delegation testing for each new gTLD. Documentation on the requirement can be referenced in Module 5 of the Draft Application Guidebook. As in the original malicious conduct memo, Specification 6 of version 3 of the Registry Agreement contains language regarding DNSSEC (see below). The first sentence of Section 6 version 3 has been modified to read "Registry Operator shall sign its TLD zone files implementing Domain Name System Security Extensions ("DNSSEC")".

  NOTE: RFC 4310 (as mentioned below) has been updated to RFC 5910.

3 Prohibition on Wild Carding

- ### Current Status and/or Updates

  The language related to the prohibition of DNS wildcards remains part of Specification 6 of version 3 of the Registry Agreement (see "Status from Original Malicious Conduct Memo" below). In addition, ICANN released an explanatory memorandum titled "Harms

and Concerns Posed by NXDOMAIN Substitution (DNS Wildcard and Similar Technologies) at Registry Level" on 24 November 2009. This explanatory memorandum describes the harms and concerns posed by NXDOMAIN substitution (commonly implemented by the use of DNS wildcard) at the registry level. The paper is a collection of the findings published by experts on the subject. The actual memorandum can be referenced at the following link:

http://www.icann.org/en/announcements/announcement-2-24nov09-en.htm

The ICANN Board of Directors resolved that new top-level domains should not use DNS redirection and synthesizing of DNS responses at its public meeting in Sydney in June 2009.

In response to the Board resolution, ICANN staff included a prohibition against redirection and synthesizing of DNS responses in the draft Registry Agreement for new gTLDs. ICANN also included a similar commitment as part of the request for new IDN ccTLDs in the proposed Terms and Conditions and in the three proposed relationship options between ICANN and the IDN ccTLD manager.

Finally, the Board also directed ICANN staff to report on the harms and concerns posed by the use of redirection and synthesizing of DNS responses, collectively, NXDOMAIN substitution.

4 Encourage removal of Orphan Glue records

- ### Current Status and/or Updates

SSAC has formed a working group to study this issue. The working group is currently examining zone files for all current gTLDs to census orphaned name servers and, if possible, to determine the extent to which these orphans are used for malicious or criminal purposes. 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 mentioned in the original malicious conduct memo, Registries must provide a description of how they will remove orphan glue records at the time a name server is removed from the zone (see below).

5 Requirement for Thick WHOIS

- ### Current Status and/or Updates

The recommendation to make "thick WHOIS" a requirement for all new gTLDs is now in place. All new gTLDs will have to implement thick WHOIS requirements, per the latest Registry Agreement.

In addition, a new clause regarding WHOIS "search ability" has been provisionally added for comment into the draft registry agreement. The clause contains the following language:

"In order to assist complainants under the UDRP to determine whether a pattern of "bad

faith" has been demonstrated by a particular registrant, WHOIS information will be available on a publicly accessible database, subject to applicable privacy policies, which will be searchable by domain name, registrant's name, registrant's postal address, contacts' names, Registrars Contact IDs and Internet Protocol address without arbitrary limit. In order to provide an effective WHOIS database, Boolean search capabilities may be offered."

The clause provides an additional tool to those involved in identifying and confronting malicious conduct in the namespace, providing that the methods and standards used to perform searches have a control structure designed to reduce the malicious use of the searching capability itself. This clause exists in some current registry agreements (.ASIA, .MOBI, .POST) and is included in this draft of the new gTLD registry agreement for discussion. As a point of reference, .NAME (http://www.icann.org/en/tlds/agreements/name/appendix-05-15aug07.htm) has had an "extensive WHOIS" searching function available since its inception. The searching function is based on a tiered access model that helps reduce the potential malicious use of the function. Comment is invited in particular on how this requirement could help address certain types of malicious conduct, and on alternate solutions whereby use of Whois data for registered names can be an effective tool in the context of mitigating malicious conduct in new gTLDs. If the requirement is supported, suggestions on development a uniform technical specification for the search function exists are also sought.

6 Centralization of zone-file access

- **Current Status and/or Updates**

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 create a proposal for a mechanism to support the centralization of access to zone files. The ZFA AG has completed its work on the strategy proposal, which can be referenced at the following link:

http://www.icann.org/en/topics/new-gtlds/zfa-strategy-paper-12may10-en.pdf

The next step for the centralization of zone file access is to implement the recommendations outlined in the proposal.

7 Documented Registry Level Abuse Contact and Policies

- **Current Status and/or Updates**

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 (see below).

8 Participation in an expedited registry security request process

- **Current Status and/or Updates**

As per the brief in the original malicious conduct memorandum, ICANN released an explanatory memorandum titled "Expedited Registry Security Request Process Posted" (see below). This explanatory memorandum defines a process called "The Expedited Registry Security Request" (ERSR) process. It 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 of the Registry Agreement for the time period necessary to respond to the Incident.

The ERSR web-based submission procedure is now available and can be referenced in Appendix A, or via the following link:

http://www.icann.org/en/registries/ersr/.

This new 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. For the sake of DNS stability, this process went live immediately on 1st October 2009. Additional information about the ERSR process can be accessed at the following link:

http://www.icann.org/en/announcements/announcement-01oct09-en.htm

9 Draft framework for high security zones verification

- **Current Status and/or Updates**

The recommendation to create a draft framework for high security zone verification was recommended by the Banking and Financial stakeholder groups such as BITS, 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 has formed the High Security Zone Top Level Domain Advisory Group ("HSTLD AG). The HSTLD AG's mandate is 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 TLD's that elect to participate in such a program.

The HSTLD AG currently consists of members of the community that have expressed an interest in assisting with the program, as well as individuals who are subject matter experts in disciplines related to the program (e.g., security, auditing, certification programs, financial services representatives) supported by members of ICANN staff. The HSTLD AG

meets regularly to build upon the concepts introduced in the original October 2009 paper, draft control elements and program requirements, and plans to publish an actionable program for community consideration and review. The HSTLD AG conducts its activities and program development through an open and transparent process. Additional information including group participants and recordings of the HSTLD AG weekly meetings are available at the following link:

http://www.icann.org/en/topics/new-gtlds/hstld-program-en.htm

The program will not be operated by ICANN. An independent entity will establish criteria and certify TLDs according to those criteria. They will be charged with monitoring and renewing certifications as well as publishing certifications.

Appendix A

Expedited Registry Security Request Process

The Expedited Registry Security Request (ERSR) has been developed to provide a process for gTLD registries who inform ICANN of a present or imminent security incident (hereinafter referred to as "Incident") to their TLD and/or the DNS to request a contractual waiver for actions it might take or has taken to mitigate or eliminate an Incident. A contractual waiver is an exemption from compliance with a specific provision of the Registry Agreement for the time period necessary to respond to the Incident. The ERSR has been designed to allow operational security to be maintained around an Incident while keeping relevant parties (e.g., ICANN, other affected providers, etc.) informed as appropriate.

An Incident could be one or more of the following:

- Malicious activity involving the DNS of scale and severity that threatens systematic security, stability and resiliency of a TLD or the DNS;
- Unauthorized disclosure, alteration, insertion or destruction of registry data, or the unauthorized access to or disclosure of information or resources on the Internet by systems operating in accordance with all applicable standards;
- An occurrence with the potential to cause a temporary or long-term failure of one or more of the critical functions of a gTLD registry as defined in ICANN's gTLD Registry Continuity Plan [PDF, 96K].

The ERSR is exclusively for Incidents, i.e., requiring immediate action by the registry and an expedited response within 3 business days from ICANN. This process is not intended to replace requests that should be made through the Registry Services Evaluation Policy (RSEP).

It is recognized that in some extraordinary instances registries may be required to take immediate action to prevent or address an Incident. In cases of such Incidents, registries should submit an ERSR as soon as possible so ICANN may respond with a retroactive wavier if appropriate.

Registries can submit an ERSR by completing a request form found at http://www.icann.org/cgi/registry-sec. The submitted request is processed as follows:

- The ERSR will automatically be forwarded to the ICANN Security Response Team and a copy will be provided to the requestor. The Security Response Team includes staff from the following departments: Security, gTLD Registry Liaison, General Counsel and Compliance.
- On a case-by-case basis, a designated member of The Security Response Team shall be responsible for contacting the Registry within 1 business day to confirm the Incident and request if necessary additional information.

- The Security Response Team may request additional information if necessary to review and consider the ERSR and the requestor will be asked to provide such information expeditiously.
- The Security Response Team will convene within 2 business days of the receipt of the request (and any requested additional information) to review and determine a response.
- ICANN will respond verbally and in writing within 3 business days of receipt of the ERSR to the requestor or their designated representative.
- A designated member of the Security Response Team will maintain contact with the Registry primary contact throughout the duration the Incident.
- If the request is received after the Registry has responded to an Incident, ICANN will endeavor to respond within 10 business days to provide in writing a retroactive waiver to the request if appropriate.
- Following a response to an ERSR, the Security Response Team in collaboration with the affected registry will develop an After-Action Report (AAR) that may be made available to the community. If an AAR is to be published, ICANN and the affected registry will jointly review which sections of the ERSR request and AAR should be redacted to ensure confidential and proprietary information is protected. ICANN and the registry can redact such information it reasonably considers confidential or proprietary.