New gTLD Program
Explanatory Memorandum

Mitigating Malicious Conduct

Date of Publication: 3 October 2009

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/topics/new-gtld-program.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 of Key Points in this Paper

ICANN seeks comments on the proposal to add specific measures to the new gTLD registry agreement, described below, to be required of all registries in order to mitigate potential malicious conduct.

During its study of malicious conduct, ICANN staff solicited and received comments from multiple outside sources, including the Anti Phishing Working Group (APWG), 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 in new gTLD registry agreements. These recommended measures are intended to increase benefits to overall security and stability for registrants and trust by all users of these new gTLD zones.

The comments received on version 2 of the Draft Applicant Guidebook, during the Sydney meeting and in the consultations since Sydney recommended measures and controls to mitigate malicious conduct be incorporated as requirements into the draft base registry agreement for new gTLDs. The following is a summary of the input considered and the process followed in preparing these recommendations.

The recommendations provide concrete mitigations of the risks of malicious conduct in nine areas:

1. Vetted registry operators
2. Demonstrated plan for DNSSEC deployment
3. Prohibition of wildcarding
4. Removal of orphan glue records when a name server entry is removed from the zone
5. Requirement for thick Whois records
6. Centralization of zone-file access
7. Documented registry level abuse contacts and procedures
8. Participation in an Expedited Registry Security Request process
9. Draft Framework for High Security Zones Verification

Together, we believe these measures will greatly help to mitigate the risk increasing malicious conduct arising from new gTLDs. Policy work on these issues and the steps taken to mitigate malicious conduct will continue. ICANN may also explore the formation of a working group combining members within the security industry and ICANN community to help develop and assess solutions and specific implementations of proposed mitigation measures.

Preface

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 many governments and other stakeholders, has been to promote competition in the domain-name marketplace while ensuring Internet security and stability. The expansion will engender innovation, choice and positive change for the Internet's addressing system. In a world with 1.5 billion Internet users diversity, choice and competition are key to the continued success and reach of the global network.

The decision to launch these new gTLD application rounds followed a detailed and lengthy consultation process with all constituencies of the global Internet community. Representatives from a wide variety of stakeholders—governments, individuals, civil society, business and intellectual property constituencies, and the technology community—were engaged in discussions for more than 18 months. In October 2007, the Generic Names Supporting Organization (GNSO)—one of the groups that coordinate global Internet policy at ICANN—completed its policy development work on new gTLDs and approved a set of recommendations. The culmination of this policy development process was a decision by the ICANN Board of Directors to adopt the community-developed policy in June 2008 at the ICANN meeting in Paris. A thorough brief to the policy process and outcomes can be found at http://gnso.icann.org/issues/new-gtlds/.

This paper is one of a series of papers that will serve as explanatory memoranda published by ICANN to assist the Internet community to better understand the Request for Proposal (RFP), also known as Applicant Guidebook. A public comment period for the Applicant Guidebook and these papers will inform a detailed review and amendment of these ideas. Those comments will be used to revise the documents in preparation of a final Applicant Guidebook.

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.

Community Input regarding the Malicious Conduct Issue

ICANN has received numerous public comments spanning multiple areas in response to its announcement proposing an expansion of the TLD space to delegate new TLDs, including IDN TLDs. One of the issues identified by several parties was the potential for increased malicious conduct that might arise from new gTLDs. In order to address this issue, ICANN sought comment from experts in responding to malicious conduct and from stakeholders impacted by malicious conduct in existing gTLDs.

The input received on the earlier versions 1 and 2 of the Draft Applicant Guidebook serve as an important primary source in the development of the recommendations being included in version 3 of the Draft Applicant Guidebook.

A second source of input on this issue is the body of reports issued by SSAC on forms of malicious conduct. Specifically, SAC038: Registrar Abuse Point of Contact (pdf) and SAC040: Measures to Protect Domain Registration Services Against Exploitation or Misuse (pdf). These reports and other work performed by the SSAC provide guidance regarding

security best practices for registries and registrars, which have guided the proposed changes in the Draft Applicant Guidebook and new gTLD registry agreement.

A third source is the draft report prepared by the Anti-Phishing Working Group (APWG), an industry association focused on eliminating the identity theft and fraud that result from the growing problem of phishing and email spoofing. This report was coordinated by the APWG's Internet Policy Committee (IPC), which includes over 90 members representing the full spectrum of the APWG's membership. It is worth noting that many ICANN stakeholders, including gTLD and ccTLD registries and registrars, Internet service providers, intellectual property owners and security and financial institutions are APWG and APWG IPC members, see http://www.antiphishing.org/sponsors.html. The APWG's IPC views the planned expansion of gTLDs to be an important event with potential impact on the e-crime space. The APWG IPC report provides comprehensive and constructive input to ICANN on numerous malicious conduct issues that the APWG's IPC feel merit attention and planning during the rollout of the new gTLDs.

A fourth source of input was provided by the Registry Internet Safety Group (RISG), a global group of responsible Internet-related organizations who work collaboratively to combat Internet identity theft, particularly phishing and malware distribution. The RISG report (pdf) provides an enumeration of several issues, which may result from an increase in the number of registries.

A fifth source of input received on the malicious conduct issue is a series of comments received from the Banking and Finance community. A set of industry associations including the BITS Fraud Reduction Program, American Banking Association, Financial Services Information Sharing and Analysis Center (*FS-ISAC*) and the Financial Services Technology Consortium (FSTC) contributed their expertise. With their unique perspective and experience in securing both networks and sensitive data, this community provided specific valuable recommendations for measures that registries should implement, including the adoption of secure business practices, to increase user trust and to reduce the risk of compromise by malicious attack.

A sixth source of input on measures to mitigate malicious conduct within new gTLDs is the work done by the Implementation Recommendation Team (IRT). While ICANN has identified trademark protection and potential for malicious abuse as separate overarching issues to be addressed in the establishment of new gTLDs, a significant intersection exists in the remediation approaches that are proposed to address these concerns. The IRT work was summarized in the "Open Letter from the IRT Introducing our Work," dated 29 May 2009. The IRT was formed by ICANN's Intellectual Property Constituency in accordance with the 6 March 2009 ICANN Board resolution (link) at the request of the community seeking solutions for potential risks to trademark holders in the implementation of new gTLDs. The report provided by the IRT team (pdf) reflects the experiential and geographic diversity of its 18 members and two alternates.

Additional sources of input come from members of the Internet security first responder community. Members of organizations such as the worldwide Forum of Incident Response and Security Teams (FIRST), which consists of the computer and network emergency response teams from 180 corporations, government bodies, universities and other institutions spread across the Americas, Asia, Europe and Oceania and help lead the world's efforts to combat cyber-crime, provided valuable advice. Members of various law enforcement agencies provided assistance by defining issues of importance

and suggestion for changes in registry operations, which would assist in combating Internet- based crime.

In addition to the sources already cited, ICANN incorporated input from participants in public consultations held in Sydney, New York, London, Hong Kong and Abu Dhabi. These consultations included dedicated sessions focused on the issue of mitigating the potential for malicious conduct and new gTLDs.

ICANN maintains a wiki on the icann.org website dedicated to the soliciting potential solutions for addressing malicious conduct in new gTLDs. The reports referenced above have been posted to this wiki and public participation and comment was invited.

Key Issues Identified

A number of issues relating to the potential for malicious conduct were identified by this diverse set of participants in the ICANN process. Although many of the issues expose unique and complex technical vulnerabilities and require a variety of controls and considerations, they can be summarized under the following key subject categories:

A. How do we ensure that bad actors do not run Registries?

Sources have asked that ICANN take steps to reduce the risk that an expanded number of registries could lead to unreliable operators or criminals entering the community and enabling malicious conduct to occur.

B. How do ensure integrity and utility of registry information?

Sources encourage ICANN to take advantage of the creation of new gTLDs to improve the quality of domain name registration and domain name resolution services in a manner that would limit opportunities for malicious conduct.

C. How do we ensure more effective effort to combat identified abuse?

Given that malicious conduct already exists and affects all TLDs, sources have called for ICANN to pursue within the establishment of new TLDs improvements to the processes and tools available to reduce on-going cyber-crime and abuse of the DNS and domain registration systems.

D. How do we provide an enhanced control framework for TLDs with intrinsic potential for abuse?

Certain new TLDs may involve e-service transactions requiring a high-confidence infrastructure (e.g., electronic financial services or e-voting) and may involve critical assets and infrastructure (such as those supporting energy infrastructures or medical services) that must be afforded increased protection from the actors already conducting malicious conduct using the domain name system. Sources have recommended ICANN take steps to create a system to enable enhanced trust in operations of such zones.

Proposed Mitigation Measures:

In order to address the malicious conduct issues summarized above, ICANN believes that a combination of measures should be taken as part of the planned implementation of new gTLDs. In addition to increased obligations on the part of new gTLD registries in their contracts with ICANN, these new registries are encouraged to negotiate stronger

standards for business and security practices with accredited registrars. Specifically, a new gTLD registry will have the ability to require registrars to implement specific measures to reduce malicious conduct in order to register labels within their zone.

Additionally, ICANN will continue to work with the community to complement existing policy development and working group efforts to address mitigation measures that to be implemented at the registrar-registrant interface.

The following are the general categories of proposed mitigation steps to be implemented in the current version of the Draft Applicant Guidebook:

1. Vetted registry operators
2. Demonstrated plan for DNSSEC deployment
3. Prohibition of wildcarding
4. Removal of orphan glue records when a name server entry is removed from the zone
5. Requirement for thick WHOIS records
6. Centralization of zone-file access
7. Documented registry level abuse contacts and procedures
8. Participation in an Expedited Registry Security Request process
9. Draft Framework for High Security Zones Verification

Relationship of issues to mitigation measures

A. How do we ensure that bad actors do not run Registries?

1. Vetted Registry Operators

B. How do ensure integrity and utility of registry information?

2. Require DNSSEC deployment
3. Prohibition on Wild Carding
4. Encourage removal of Orphan Glue records

C. How do we ensure more focused efforts on combating identified abuse?

5. Requirement for Thick WHOIS
6. Centralization of zone-file access
7. Documented Registry & Registrars level abuse contact and policies
8. Availability of Expedited Registry Security Request process

D. How do we provide an enhanced control framework for TLDs with intrinsic potential for malicious conduct?

9. High Security Zones Verification Program

Specific Measures to be implemented in new Registry Contracts

The following measures are included in the Applicant Guidebook and reflect procedures

required of all new registries. The location of language within the draft Applicant Guidebook is identified. A brief description of the rationale for each specific measure is included (in italics).

1. Vetted Registry Operators

Applicant question (attachment to Module 2) states:

ICANN may deny an otherwise qualified application for any of the following reasons:

Applicant, or any officer, partner, director, or manager or other affiliate, or any person or entity owning (or beneficially owning) fifteen percent or more of applicant:

a. within the past ten years, has been convicted of a felony or of a misdemeanor related to financial or corporate governance misconduct, or has been judged by a court to have committed fraud or breach of fiduciary duty, or has been the subject of a judicial determination that ICANN deemed as the substantive equivalent of any of the above;

b. within the past ten years, has been disciplined by any government or industry regulatory body for conduct involving dishonesty or misuse of the funds of others;

c. is currently involved in any judicial or regulatory proceeding that could result in a conviction, judgment, determination, or discipline of the type specified in (a) or (b);

d. is the subject of a disqualification imposed by ICANN which is in effect at the time the application is considered; or

e. f ail to provide ICANN with the identifying information necessary to confirm identity at the time of application

f. is the subject of a pattern of decisions indicating liability for, or repeated practice of bad faith in regard to domain name registrations, including:

(i) acquiring domain names primarily for the purpose of selling, renting, or otherwise transferring the domain name registrations to the owner of a trademark or service mark or to a competitor, for valuable consideration in excess of documented out-of-pocket costs directly related to the domain name; or

(ii) registering domain names in order to prevent the owner of the trademark or service mark from reflecting the mark in a corresponding domain name; or

(iii) registering domain names primarily for the purpose of disrupting the business of a competitor; or

(iv) using domain names with intent to attract, for commercial gain, Internet users to a web site or other on-line location, by creating a likelihood of confusion with a trademark or service mark as to the source, sponsorship, affiliation, or endorsement of the web site or location or of a product or service on the web site or location.

Note: Information gathered during the course of these background checks including records of past criminal activity will be considered during the application process.

The application process will include standardized, thorough background and reference checks for companies and individuals (e.g., key officers). This step will mitigate the risk that known felons, members of criminal organizations or those with histories of bad business operations will become involved in registry operations or gain ownership or proxy control of registries.

2. Require DNSSEC deployment

Registry Operators will be required to provide a documented plan to sign their zone file and have DNSSEC implementation in place at start of operations.

The following language has been added to Specification 6 of version 3 of the Registry Agreement, subject to technical review:

"Registry Operator shall implement Domain Name System Security Extensions ("DNSSEC"). During the Term, Registry Operator shall comply with RFCs 4033, 4034, 4035, 4509 and 4310 and their successors, and follow the best practices described in RFC 4641 and its successors. If Registry Operator implements Hashed Authenticated Denial of Existence for DNS Security Extensions, it shall comply with RFC 5155 and its successors. Registry Operator shall accept public-key material from child domain names in a secure manner according to industry best practices. Registry shall also publish in its website the practice and policy document (also known as the DNSSEC Policy Statement or DPS) describing key material storage, access and usage for its own keys and the registrants' trust anchor material."

The advantages provided by implementation of DNSSEC to overall security, and stability of the Internet are well documented. ICANN is committed to the signing of the root zone within 2009 and will ensure that the establishment of new gTLDs enables the use of this important means for improving DNS security.

3. Prohibition on Wild Carding

The SAC041 report by the SSAC (approved by the ICANN Board) and reports by other commenting organizations have advised ICANN that new TLDs should be prohibited from using DNS redirection and synthesized DNS responses.

Given the current trend of malware associated with sites serving advertisements, the redirection of domains to advertising sites presents the potential for increased malicious conduct. For domain names which are either not registered by a Registrant, or the Registrant has not supplied valid records such as NS records for listing in the DNS zone file, or their status does not allow them to be published in the DNS, the use of DNS wildcard Resource Records as described in RFC 4592 or any other method or technology for synthesizing DNS Resources Records or using redirection within the DNS by the Registry is forbidden. Specifically, when queried for such domain names the authoritative name servers must return a "Name Error" response (also known as NXDOMAIN), RCODE 3 as described in RFC 1035 and related RFCs.

This provision applies for all DNS zone files at all levels in the DNS tree for which the Registry Operator (or an affiliate engaged in providing Registration Services) maintains data, arranges for such maintenance, or derives revenue from such maintenance.

The following prohibition on wildcards has been added to Specification 6 of version 3 of the Registry Agreement:

"For domain names which are either not registered by a registrant, or the registrant has not supplied valid records such as NS records for listing in the DNS zone file, or their status does not allow them to be published in the DNS, the use of DNS wildcard Resource Records as described in RFC 4592 or any other method or technology for synthesizing DNS Resources Records or using redirection within the DNS by the Registry is prohibited. When queried for such domain names the authoritative name servers must return a "Name Error" response (also known as NXDOMAIN), RCODE 3 as described in RFC 1035 and related RFCs. This provision applies for all DNS zone files at all levels in the DNS tree for which the Registry Operator (or an affiliate engaged in providing Registration Services) maintains data, arranges for such maintenance, or derives revenue from such maintenance."

The SAC041 report (pdf) by the SSAC and reports by other commenting organizations have advised ICANN that new TLDs should be prohibited from using DNS redirection and synthesized DNS responses. The dangers inherent in redirection and synthesized responses not only in TLDs but also at subordinate levels of the DNS. This provision in new registry contracts is designed to address this issue at the registry level.

4. Encourage removal of Orphan Glue records

As part of their published anti-abuse policies, registries must provide a description of how it will remove orphan glue records at the time a name server entry is removed from the zone. The following is excerpted from the Draft Application Guidebook, module 2 applicant questions:

"Abuse Prevention and Mitigation: Applicants should describe the proposed policies and procedures to minimize abusive registrations and other activities that have a negative impact on Internet users… Answers should include a rapid takedown or suspension system, and *proposed measures for management and removal of orphan glue records for names removed from the zone*."

An APWG study estimated that approximately 3% of domains used for phishing were using "orphan name server" records, i.e. remnants from a domain that was previously removed from a registry. This can create a potential "safe haven" name server entry in that TLD's zone file that abusers can use to support criminal domain registrations.

5. Requirement for Thick WHOIS

The Registry Operator must maintain and provide public access to registration data using a thick Whois data model as required by Specification 4 to version 3 of the form registry agreement.

"WHOIS Service**.** Until ICANN specifies a different format and protocol, Registry Operator will operate a registration data publication service available via both port 43 and a website at <whois.nic.(TLD)> in accordance with RFC 3912 providing free public query-based access to at least the following elements in the following format. ICANN reserves the right to specify alternative formats and protocols, including the Internet Registry Information Service ("IRIS" – RFC 3981 and related RFCs), and upon such specification, the Registry Operator will implement such alternative specification as soon as reasonably practicable."

ICANN has proposed modification of the Whois requirements in the proposed new

registry agreement to require all registries to offer thick Whois output as described in a previous explanatory memorandum (pdf). In addition, the draft report (pdf) of the Implementation Recommendations Team formed by ICANN's Intellectual Property Constituency states "the IRT believes that the provision of WHOIS information at the registry level under the Thick WHOIS model is essential to the cost-effective protection of consumers and intellectual property owners." Implementation of Thick WHOIS will help mitigate malicious conduct by ensuring greater accessibility and improved stability of records access.

6. Centralization of zone-file access

ICANN will require that registries allow access to zone file data for the purpose of making it available through a centralized provider.

A suggested or proposed version of Specification 4 of the Registry Agreement (subject to technical review) provides that the registry operator will make such data available to the community generally:

"2.2.1. General Access. Registry Operator shall provide bulk access to the zone files for the registry for the TLD to ICANN or its designee on a continuous basis in the manner ICANN may reasonably specify from time to time.

"2.2.2. Central Zone File Depository. In the event that ICANN or its designee establishes a central zone file depository, Registry Operator will provide all zone file data to ICANN or to a third party operator of such depository designated by ICANN upon request by ICANN. Should such central zone file depository be established, ICANN may waive, at ICANN's sole discretion, compliance with Section 2.1 of this Specification 4. [This Section 2.2.2 is included for community discussion purposes as a result of prior community discussions regarding mitigation of malicious conduct. Under this provision, an ICANN designee could take on the responsibility currently carried out by registry operators of vetting and monitoring access to zone file data by responsible parties for legitimate purposes.]"

In order to facilitate access to registry zone file data, which is currently handled by individual registries ICANN (or party designated by ICANN to perform this function) would collect zone file data from new gTLD registries and provide subscribers electronic access to the data. This would also include a single contract to sign for parties desiring access to the zone files for ICANN-regulated registries ICANN would set-up the access contracts based on the current model, and administer/support the transfer system.

This central coordination will allow the anti-abuse community to efficiently obtain updates on new domains as they are created within each zone.

7. Documented Registry & Registrars Level Abuse Contact and Policies

Registry Operator shall provide a single abuse point of contact for all domains within the TLD. This abuse contact will be responsible for addressing and providing timely response to abuse complaints received from recognized parties, such as other registries, registrars, law enforcement organizations and recognized members of the anti-abuse community. Registries must also provide a description of their policies to combat abuse.

Registry Operator may require of all registrars with whom they contract for services that they provide an abuse point of contact. This step is consistent with recommendations of

the SSAC report SAC038 (pdf). Registries may also require registrars to publish a documented abuse policy that is consistent with the Registry's abuse policy. At both levels, the policy addresses the procedures by which it will:

1. suspend domains identified as being involved in trademark abuse, phishing, willful distribution of malware or other illegal or fraudulent activity
2. address issues relating to resellers or other distributors of services under their control
3. remove orphan glue records associated with malicious conduct
4. identify the abuse point of contact and how communications with that point of contact are expected to occur

The following language has been added to Specification 6 of version 3 of the Registry Agreement to address this point:

"Registry Operator shall provide on its website its accurate contact details including a valid email and mailing address as well as a primary contact for handling inquires related to malicious conduct in the TLD, and will provide ICANN with prompt notice of any changes to such contact details."

In addition, he following excerpt from a module 2 question is included in the Draft Application Guidebook, version 3:

"… Each registry operator will be required to establish and publish on its website a single abuse point of contact responsible for addressing matters requiring expedited attention and providing a timely response to abuse complaints concerning all names registered in the TLD through all registrars of record, including those involving a reseller."

The implementation of new registries, possibly on a large scale, necessitates new, well-defined controls and defined roles in the domain registration process. Abuse contacts and policies at both registry and registrar levels will be a fundamental step in allowing future efforts to combat malicious conduct to continue and scale with the addition of new operators.

8. Availability of Expedited Registry Security Request Process

ICANN has developed an additional procedure http://www.icann.org/en/announcements/announcement-01oct09-en.htm, in consultation with gTLD registries, registrars and security experts, based on lessons learned in responding to the Conficker worm, to provide a process for registries to inform ICANN of a present or imminent security situation involving a gTLD and to request a contractual waiver for actions the registry might take or has taken to mitigate or eliminate the security concerns.

A security situation is defined as one or more of the following:

a. Malicious activity involving the DNS of scale and severity that threatens systematic security, stability and resiliency of the DNS;

b. Potential or actual 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;

c. Potential or actual undesired consequences that may cause or threaten 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).

The ERSR is exclusively for Incidents that require immediate action by the registry and an expedited response (within 24-48 hours) from ICANN. This process is not intended to replace requests that should be made through the Registry Services Evaluation Policy (RSEP) (link).

9. High Security Zones Verification Program

In order to facilitate the overall community need for enhanced trust within select gTLD's, ICANN has created a draft framework for a gTLD verification program. As currently proposed, this verification program will be entirely optional.

A choice not to pursue verification at the time of new gTLD application does NOT reflect negatively on the applicant, nor affect its scores in the evaluation process. The purpose of the verification program is to set an acceptable set of standards and criteria that will enhance trust in a verified gTLD, through the application of appropriate operational and security controls and measuring that the gTLD registries and registrars performance against the controls. gTLD registries that elect to pursue verification will be able to demonstrate verification through some method of public display, such as a "seal" or a mark that is verifiable with a master list of verified gTLD's. ICANN will maintain and publish the master list of verified gTLDs.

In addition to maintaining the master list of verified gTLD's, ICANN's role in the program is to help set, refine and manage the governance of the program, and to work with the community to establish program standards and criteria. Actual assessment of a gTLD against the program standards and criteria will be performed by independent entities.

To achieve verification under the proposed program, the registry operations must be consistent with the following principles (see Guidebook, module 2):

a. The registry demonstrates that the operator maintains effective controls to provide assurance that the security, availability, confidentiality, and privacy of systems and information assets supporting critical registry IT and business operations is maintained.

b. The registry maintains effective controls to provide assurance that the processing of core registry functions is authorized, accurate, complete, and performed in a timely manner in accordance with established policies and standards. The identity of participating entities are established and authenticated.

c. The registry maintains effective controls to provide reasonable assurance that the processing of core registrar functions by its registrars is 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 processes required to achieve verification include verification of both registry operations and supporting registrar operations.

In the event that an applicant wishes to apply for the verification option, it does so in a two-phased process.

Phase I

Prior to delegation of the new gTLD, the applicant participates in an assessment, which will include the following:

- Background information
- Domain management/takedown procedures
- Abuse point of contact and response
- Procedures for escrow of records

After the new gTLD has been delegated and begins operations, a specified period will be given for the applicant to implement all the pre-approved processes and controls.

Phase II

The next phase tests the processes, controls, and procedures documented in Phase I to validate that they are operating as planned. If deficiencies are identified, they will be communicated to ICANN by the independent assessment agency. The registry operator will have defined period to resolve the problem before the applicant's request for verification will be denied. The registry operator may re-apply for verification at a later time.

In the event that any new gTLD registry application completes the evaluation and the TLD is delegated, the registry operator may choose at that point to apply for verification and would then complete the above tests in a single phase. That is, an applicant may choose to take the steps to obtain verification after it has completed the evaluation process and is operating its new gTLD, rather than concurrently with the evaluation process.

The controls necessary to support verification are assessed through audit on a periodic basis, to retain the gTLD's verified status.

ICANN believes that this verification program allows for an enhanced level of trust within the certified gTLDs, at the expense of additional requirements for establishing the accuracy of controls for registry, registrar and registrant processing as well as registry and registrar operations. The balance between trust and cost/benefit constitutes the key business decision that a gTLD registry will use as the basis to determine if verification is an appropriate business process to pursue.

The Verification Program applies to a proposed set of activities necessary to support an enhanced channel of trust for registry operations. The focus of the draft framework is on the controls necessary to reduce the potential for malicious conduct within gTLD registries that elect to pursue a verification seal from ICANN. The scope is limited to the controls and activities at the registry and registrar operations level and does not extend to the operations of registrants. The Verification Program is intended to provide reasonable, but not absolute, assurance that the verified gTLD's have effective operating controls that meet the verification criteria. The establishment of the verification criteria and periodic independent review/audit of their effectiveness through the Verification Program will therefore provide an increased level of trust.