GAC Advice Response Form for Applicants

The Governmental Advisory Committee (GAC) has issued advice to the ICANN Board of Directors regarding New gTLD applications. Please see Section IV, Annex I, and Annex II of the GAC Beijing Communique for the full list of advice on individual strings, categories of strings, and strings that may warrant further GAC consideration.

Respondents should use this form to ensure their responses are appropriately tracked and routed to the ICANN Board for their consideration. Complete this form and submit it as an attachment to the ICANN Customer Service Center via your CSC Portal with the Subject, "[Application ID] Response to GAC Advice" (for example "1-111-11111 Response to GAC Advice"). All GAC Advice Responses must be received no later than 23:59:59 UTC on 10-May-2013.

Respondent:

Applicant Name	.APP Registry Inc.
Application ID	1-1013-7451
Applied for TLD (string)	APP

Response:

Dear ICANN Board & GAC,

First and foremost, .APP Registry Inc. thanks the GAC for providing a comprehensive set of advice to the ICANN Board on the subject of safeguards for new gTLDs. We also appreciate the opportunity to provide our response and feedback to the ICANN Board.

As a responsible new gTLD applicant, .APP Registry Inc. is glad to say that it has already included many measures in the submitted proposal to address the issues raised by the GAC, and believe that its proposal is compliant with the GAC advice. We further remain fully prepared to work closely with the GAC and GAC members on any area to further enhance the safeguard measures for the governance and management of the introduction and operations of the .APP gTLD in an orderly, secure and stable manner, technically and socially.

As a participant in the ICANN process, we are encouraged by the active participation of the GAC in the process. The GAC and governments are an important component of the ICANN process and the multi-stakeholder governance of the Internet's root DNS. Many of the issues raised by the GAC advice are issues that are actively discussed by the ICANN community. Some of which are already included in the considerations for this round of new gTLDs (e.g. #28 Abuse Prevention and Mitigation), some others are currently being discussed within the ICANN process. For example, policy development processes for WHOIS are ongoing and registration

and usage abuse issues continue to be examined, including especially where such abuse issues should be within or beyond the scope of ICANN's purview.

For such items, we understand that ongoing multi-stakeholder processes should not be circumvented, and remain diligent against such undermining. Nevertheless, we are fully prepared to improve on our proposed mechanisms in our application as well as to implement appropriate measures for.APP specifically as Registry policies before community wide ICANN policies are fully in place.

Finally, we also bring your attention to the ongoing work underway since the recent CEO Roundtables and further discussed at the DNS Summit (http://blog.icann.org/2013/04/dns-summit-in-new-york/). Especially the "proposals to codify ethical standards for DNS businesses", which may be an appropriate framework for addressing issues (e.g. content related) that may be beyond the scope of ICANN's policy mandate.

Attached further are specific responses to each of the issues raised in the GAC advice with excerpts from particular sections of the submitted .APP Registry Inc. proposal (https://gtldresult.icann.org/application-result/applicationstatus/applicationdetails:downloadapplication/457?t:ac=457) and how it complies with and relates to the GAC advice.

We look forward to continuing the dialogue with the ICANN board and the GAC to address any issues and put policies in place to mitigate against concerns in a constructive and prompt manner.

Sincerely,

.APP Registry Inc.

GAC Advice Response Form for Applicants

.APP. Response to GAC Communiqué – Beijing April 11, 2013

Annex I

Safeguards on New gTLDs

The GAC considers that Safeguards should apply to broad categories of strings. For clarity, this means any application for a relevant string in the current or future rounds, in all languages applied for.

The GAC advises the Board that all safeguards highlighted in this document as well as any other safeguard requested by the ICANN Board and/or implemented by the new gTLD registry and registrars should:

• be implemented in a manner that is fully respectful of human rights and fundamental freedoms as enshrined in international and, as appropriate, regional declarations, conventions, treaties and other legal instruments – including, but not limited to, the UN Universal Declaration of Human Rights.
• respect all substantive and procedural laws under the applicable jurisdictions.
• be operated in an open manner consistent with general principles of openness and non-discrimination.

Safeguards Applicable to all New gTLDs
The GAC Advises that the following six safeguards should apply to all new gTLDs and be subject to contractual oversight.

We are prepared to be subjected to contractual oversight for safeguards applicable to all new gTLDs.

1. WHOIS verification and checks — Registry operators will conduct checks on a statistically significant basis to identify registrations in its gTLD with deliberately false, inaccurate or incomplete WHOIS data at least twice a year. Registry operators will weight the sample towards registrars with the highest percentages of deliberately false, inaccurate or incomplete records in the previous checks. Registry operators will notify the relevant registrar of any inaccurate or incomplete records identified during the checks, triggering the registrar's obligation to solicit accurate and complete information from the registrant.

We are supportive of the direction for this advice and believe that we are already compliant. The scope and specific standard implementation of such policies may best be developed as a product of the ongoing WHOIS policy development process.

Nevertheless, individual Registry policies can provide the interim solution for this safeguard. We, along with our Technical Services Provider Afilias, have already

provided some of these mechanisms in our original response to #28 Abuse Prevention and Mitigation:

Methods to promote WHOIS accuracy

The creation and maintenance of accurate WHOIS records is an important part of registry management. As described in our response to question #26, WHOIS, the registry operator will manage a secure, robust and searchable WHOIS service for this TLD.

WHOIS data accuracy

The registry operator will offer a "thick" registry system. In this model, all key contact details for each domain name will be stored in a central location by the registry. This allows better access to domain data, and provides uniformity in storing the information. The registry operator will ensure that the required fields for WHOIS data (as per the defined policies for the TLD) are enforced at the registry level. This ensures that the registrars are providing required domain registration data. Fields defined by the registry policy to be mandatory are documented as such and must be submitted by registrars. The Afilias registry system verifies formats for relevant individual data fields (e.g. e-mail, and phone/fax numbers). Only valid country codes are allowed as defined by the ISO 3166 code list. The Afilias WHOIS system is extensible, and is capable of using the VAULT system, described further below.

Similar to the centralized abuse point of contact described above, the registry operator can institute a contact email address which could be utilized by third parties to submit complaints for inaccurate or false WHOIS data detected. This information will be processed by Afilias' support department and forwarded to the registrars. The registrars can work with the registrants of those domains to address these complaints. Afilias will audit registrars on a yearly basis to verify whether the complaints being forwarded are being addressed or not. This functionality, available to all registry operators, is activated based on the registry operator's business policy.

Afilias also incorporates a spot-check verification system where a randomly selected set of domain names are checked periodically for accuracy of WHOIS data. Afilias' .PRO registry system incorporates such a verification system whereby 1% of total registrations or 100 domains, whichever number is larger, are spot-checked every month to verify the domain name registrant's critical information provided with the domain registration data. With both a highly qualified corps of engineers and a 24x7 staffed support function, Afilias has the capacity to integrate such spot-check functionality into this TLD, based on the registry operator's business policy. Note: This functionality will not work for proxy protected WHOIS information, where registrars or their resellers have the actual registrant data. The solution to that problem lies with either registry or registrar policy, or a change in the general marketplace practices with respect to proxy registrations.

Finally, Afilias' registry systems have a sophisticated set of billing and pricing functionality which aids registry operators who decide to provide a set of financial incentives to registrars for maintaining or improving WHOIS accuracy. For instance, it is conceivable that the registry operator may decide to provide a discount for the domain registration or renewal fees for validated registrants, or levy a larger cost for the domain registration or renewal of proxy domain names. The Afilias system has the capability to support such incentives on a configurable basis, towards the goal of promoting better WHOIS accuracy.

Role of registrars

As part of the RRA (Registry Registrar Agreement), the registry operator will require the registrar to be responsible for ensuring the input of accurate WHOIS data by their registrants. The Registrar/Registered Name Holder Agreement will include a specific clause to ensure accuracy of WHOIS data, and to give the registrar rights to cancel or suspend registrations if the Registered Name Holder fails to respond to the registrar's query regarding accuracy of data. ICANN's WHOIS Data Problem Reporting System (WDPRS) will be available to those who wish to file WHOIS inaccuracy reports, as per ICANN policy (http://wdprs.internic.net/).

The above are the baseline abuse prevention and mitigation measures of the registry. The registry is prepared to work with ICANN and the GAC to further enhance the measures where appropriate.

2. Mitigating abusive activity — Registry operators will ensure that terms of use for registrants include prohibitions against the distribution of malware, operation of botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law.

We are prepared to and have already proposed to include in our Registry-Registrar Agreement (RRA) provisions to ensure that terms of use for registrants include prohibitions against abusive activities.

The following is an extract from our response to #28 Abuse Prevention and Mitigation:

.APP Anti-Abuse Policy
The following Anti-Abuse Policy is effective upon launch of the TLD. Malicious use of domain names will not be tolerated. The nature of such abuses creates security and stability issues for the registry, registrars, and registrants, as well as for users of the Internet in general. The registry operator definition of abusive use of a domain includes, without limitation, the following:
• *Illegal or fraudulent actions;*

• *Spam: The use of electronic messaging systems to send unsolicited bulk messages. The term applies to email spam and similar abuses such as instant messaging spam, mobile messaging spam, and the spamming of web sites and Internet forums;*
• *Phishing: The use of counterfeit web pages that are designed to trick recipients into divulging sensitive data such as personally identifying information, usernames, passwords, or financial data;*
• *Pharming: The redirecting of unknowing users to fraudulent sites or services, typically through, but not limited to, DNS hijacking or poisoning;*
• *Willful distribution of malware: The dissemination of software designed to infiltrate or damage a computer system without the owner's informed consent. Examples include, without limitation, computer viruses, worms, keyloggers, and Trojan horses.*
• *Malicious fast-flux hosting: Use of fast-flux techniques with a botnet to disguise the location of web sites or other Internet services, or to avoid detection and mitigation efforts, or to host illegal activities.*
• *Botnet command and control: Services run on a domain name that are used to control a collection of compromised computers or "zombies," or to direct distributed denial-of-service attacks (DDoS attacks);*
• *Illegal Access to Other Computers or Networks: Illegally accessing computers, accounts, or networks belonging to another party, or attempting to penetrate security measures of another individual's system (often known as "hacking"). Also, any activity that might be used as a precursor to an attempted system penetration (e.g., port scan, stealth scan, or other information gathering activity).*

We are prepared to explore to include additional safeguards where appropriate in consultation with ICANN and the GAC.

3. Security checks — While respecting privacy and confidentiality, Registry operators will periodically conduct a technical analysis to assess whether domains in its gTLD are being used to perpetrate security threats, such as pharming, phishing, malware, and botnets. If Registry operator identifies security risks that pose an actual risk of harm, Registry operator will notify the relevant registrar and, if the registrar does not take immediate action, suspend the domain name until the matter is resolved.

We are supportive of proactive measures to ensure the security and stability of the Internet. As indicated in the GAC advice, the respecting of privacy and confidentiality is paramount. Furthermore, while the inclusion of appropriate terms of use for registrants as described in "2. Mitigating abusive activity" above provides an effective enforcement mechanism, the subject matter of certain threats may traverse beyond the purview of ICANN policy coordination. For example matters concerning content. Such determination may best be addressed in proper ICANN policy development processes if implemented as a contractual and enforcement matter by ICANN.

Nevertheless, the Registry is fully prepared to implement policies within the registry and have already proposed such mechanisms in our original application under #28 Abuse Prevention and Mitigation:

Different types of malicious activities require different methods of investigation and documentation. Further, the registry operator expects to face unexpected or complex situations that call for professional advice, and will rely upon professional, trained investigators as needed.

In general, there are two types of domain abuse that must be addressed:
a) Compromised domains. These domains have been hacked or otherwise compromised by criminals, and the registrant is not responsible for the malicious activity taking place on the domain. For example, the majority of domain names that host phishing sites are compromised. The goal in such cases is to get word to the registrant (usually via the registrar) that there is a problem that needs attention with the expectation that the registrant will address the problem in a timely manner. Ideally such domains do not get suspended, since suspension would disrupt legitimate activity on the domain.
b) Malicious registrations. These domains are registered by malefactors for the purpose of abuse. Such domains are generally targets for suspension, since they have no legitimate use.

The standard procedure is that the registry operator will forward a credible alleged case of malicious domain name use to the domain's sponsoring registrar with a request that the registrar investigate the case and act appropriately. The registrar will be provided evidence collected as a result of the investigation conducted by the trained abuse handlers. As part of the investigation, if inaccurate or false WHOIS registrant information is detected, the registrar is notified about this. The registrar is the party with a direct relationship with—and a direct contract with—the registrant. The registrar will also have vital information that the registry operator will not, such as:
• Details about the domain purchase, such as the payment method used (credit card, PayPal, etc.);
• The identity of a proxy-protected registrant;
• The purchaser's IP address;
• Whether there is a reseller involved, and;
• The registrant's past sales history and purchases in other TLDs (insofar as the registrar can determine this).

Registrars do not share the above information with registry operators due to privacy and liability concerns, among others. Because they have more information with which to continue the investigation, and because they have a direct relationship with the registrant, the registrar is in the best position to evaluate alleged abuse. The registrar can determine if the use violates the registrar's legal terms of service or the registry Anti-Abuse Policy, and can decide whether or not to take any action. While the language and terms vary, registrars will be expected to include language in their registrar-registrant contracts that indemnifies the registrar if it takes action, and

allows the registrar to suspend or cancel a domain name; this will be in addition to the registry Anti-Abuse Policy. Generally, registrars can act if the registrant violates the registrar's terms of service, or violates ICANN policy, or if illegal activity is involved, or if the use violates the registry's Anti-Abuse Policy.

If a registrar does not take action within a time period indicated by the registry operator (usually 24 hours), the registry operator might then decide to take action itself. At all times, the registry operator reserves the right to act directly and immediately if the potential harm to Internet users seems significant or imminent, with or without notice to the sponsoring registrar.

The registry operator will be prepared to call upon relevant law enforcement bodies as needed. There are certain cases, for example, Illegal pharmacy domains, where the registry operator will contact the Law Enforcement Agencies to share information about these domains, provide all the evidence collected and work closely with them before any action will be taken for suspension. The specific action is often dependent upon the jurisdiction of which the registry operator, although the operator in all cases will adhere to applicable laws and regulations.

When valid court orders or seizure warrants are received from courts or law enforcement agencies of relevant jurisdiction, the registry operator will order execution in an expedited fashion. Compliance with these will be a top priority and will be completed as soon as possible and within the defined timelines of the order. There are certain cases where Law Enforcement Agencies request information about a domain including but not limited to:
- *Registration information*
- *History of a domain, including recent updates made*
- *Other domains associated with a registrant's account*
- *Patterns of registrant portfolio*

Requests for such information is handled on a priority basis and sent back to the requestor as soon as possible. Afilias sets a goal to respond to such requests within 24 hours.

The registry operator may also engage in proactive screening of its zone for malicious use of the domains in the TLD, and report problems to the sponsoring registrars. The registry operator could take advantage of a combination of the following resources, among others:
- *Blocklists of domain names and nameservers published by organizations such as SURBL and Spamhaus.*
- *Anti-phishing feeds, which will provide URLs of compromised and maliciously registered domains being used for phishing.*
- *Analysis of registration or DNS query data [DNS query data received by the TLD nameservers.]*

We are prepared to explore to include additional safeguards where appropriate in consultation with ICANN and the GAC.

4. Documentation — Registry operators will maintain statistical reports that provide the number of inaccurate WHOIS records or security threats identified and actions taken as a result of its periodic WHOIS and security checks. Registry operators will maintain these reports for the agreed contracted period and provide them to ICANN upon request in connection with contractual obligations.

We are supportive of the conceptual directive and are prepared to maintain such documentation. We however caution about misinterpretation and/or misuse of such statistical data.

As proposed in our application (under #28 Abuse Prevention and Mitigation):

The registry operator will keep records and track metrics regarding abuse and abuse reports. These will include:
- *Number of abuse reports received by the registry's abuse point of contact described above;*
- *Number of cases and domains referred to registrars for resolution;*
- *Number of cases and domains where the registry took direct action;*
- *Resolution times;*
- *Number of domains in the TLD that have been blacklisted by major anti-spam blocklist providers, and;*
- *Phishing site uptimes in the TLD.*

…

The security function includes a communication and outreach function, with information sharing with industry partners regarding malicious or abusive behavior, in order to ensure coordinated abuse mitigation across multiple TLDs.

Assessing abuse reports requires great care, and the registry operator will rely upon professional, trained investigators who are versed in such matters. The goals are accuracy, good record-keeping, and a zero false-positive rate so as not to harm innocent registrants.

We are prepared to explore to include additional safeguards where appropriate in consultation with ICANN and the GAC.

5. Making and Handling Complaints – Registry operators will ensure that there is a mechanism for making complaints to the registry operator that the WHOIS information is inaccurate or that the domain name registration is being used to facilitate or promote malware, operation of botnets, phishing, piracy, trademark or

copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law.

We are supportive of this advice ad believe that our original proposal is already compliant with the GAC advice. Description of the mechanisms for handling complaints have been included in our response to #28 Abuse Prevention and Mitigation:

Abuse point of contact and procedures for handling abuse complaints

The registry operator will establish an abuse point of contact. This contact will be a role-based e-mail address of the form "abuse@registry.APP". This e-mail address will allow multiple staff members to monitor abuse reports on a 24x7 basis, and then work toward closure of cases as each situation calls for. For tracking purposes, the registry operator will have a ticketing system with which all complaints will be tracked internally. The reporter will be provided with the ticket reference identifier for potential follow-up. Afilias will integrate its existing ticketing system with the registry operator's to ensure uniform tracking and handling of the complaint. This role-based approach has been used successfully by ISPs, e-mail service providers, and registrars for many years, and is considered a global best practice.

The registry operator's designated abuse handlers will then evaluate complaints received via the abuse system address. They will decide whether a particular issue is of concern, and decide what action, if any, is appropriate.

In general, the registry operator will find itself receiving abuse reports from a wide variety of parties, including security researchers and Internet security companies, financial institutions such as banks, Internet users, and law enforcement agencies among others. Some of these parties may provide good forensic data or supporting evidence of the malicious behavior. In other cases, the party reporting an issue may not be familiar with how to provide such data or proof of malicious behavior. It is expected that a percentage of abuse reports to the registry operator will not be actionable, because there will not be enough evidence to support the complaint (even after investigation), and because some reports or reporters will simply not be credible.

We are prepared to explore to include additional safeguards where appropriate in consultation with ICANN and the GAC.

6. Consequences – Consistent with applicable law and any related procedures, registry operators shall ensure that there are real and immediate consequences for the demonstrated provision of false WHOIS information and violations of the requirement that the domain name should not be used in breach of applicable law; these consequences should include suspension of the domain name.

We are supportive of including mechanisms to suspend a domain name against abusive activities and believe we are already compliant with the GAC advice. In our proposal (under #28 Abuse Prevention and Mitigation and #29 Rights Protection Mechanisms), we have already included mechanisms to disqualify, suspend, cancel or delete domain registrations where appropriate:

Pursuant to the Registry-Registrar Agreement, registry operator reserves the right at its sole discretion to deny, cancel, or transfer any registration or transaction, or place any domain name(s) on registry lock, hold, or similar status, that it deems necessary: (1) to protect the integrity and stability of the registry; (2) to comply with any applicable laws, government rules or requirements, requests of law enforcement, or any dispute resolution process; (3) to avoid any liability, civil or criminal, on the part of registry operator, as well as its affiliates, subsidiaries, officers, directors, and employees; (4) per the terms of the registration agreement and this Anti-Abuse Policy, or (5) to correct mistakes made by registry operator or any registrar in connection with a domain name registration. Registry operator also reserves the right to place upon registry lock, hold, or similar status a domain name during resolution of a dispute.

We are prepared to explore to include additional safeguards where appropriate in consultation with ICANN and the GAC.

Category 1 Consumer Protection, Sensitive Strings, and Regulated Markets:
The GAC Advises the ICANN Board:
• Strings that are linked to regulated or professional sectors should operate in a way that is consistent with applicable laws. These strings are likely to invoke a level of implied trust from consumers, and carry higher levels of risk associated with consumer harm. The following safeguards should apply to strings that are related to these sectors:

1. Registry operators will include in its acceptable use policy that registrants comply with all applicable laws, including those that relate to privacy, data collection, consumer protection (including in relation to misleading and deceptive conduct), fair lending, debt collection, organic farming, disclosure of data, and financial disclosures.

We are prepared to be and believe that our proposal is already compliant with this advice.

As part of our response to #28 Abuse Prevention and Mitigation, we have included provisions to ensure that registrants comply with all applicable laws:

The registry operator definition of abusive use of a domain includes, without limitation, the following:
• *Illegal or fraudulent actions;*

- *Spam;*
- *Phishing;*
- *Pharming;*
- *Willful distribution of malware;*
- *Malicious fast-flux hosting;*
- *Botnet command and control;*
- *Illegal Access to Other Computers or Networks.*

We are prepared to explore to include additional safeguards where appropriate in consultation with ICANN and the GAC.

2. Registry operators will require registrars at the time of registration to notify registrants of this requirement.

We are prepared to be and believe our proposal is compliant with this advice. The Registry will specify in its Registry-Registrar Agreement (RRA) that all registrants must be notified of this requirement at the time of registration.

3. Registry operators will require that registrants who collect and maintain sensitive health and financial data implement reasonable and appropriate security measures commensurate with the offering of those services, as defined by applicable law and recognized industry standards.

We are prepared to be and believe that our proposal is already compliant with this advice. As described in 1. above, illegal behaviour under applicable law is considered abusive activities disallowed by the registry. The Registry will have the ability to utilize the APM (Abuse Prevention & Mitigation) mechanisms to suspend, cancel, delete or otherwise take action against the domain registration.

We are prepared to explore to include additional safeguards where appropriate in consultation with ICANN and the GAC.

4. Establish a working relationship with the relevant regulatory, or industry self- --regulatory, bodies, including developing a strategy to mitigate as much as possible the risks of fraudulent, and other illegal, activities.

We are supportive of and fully prepared to be compliant with this advice.

Because of the nature of ".APP" and because it is not as much a "regulated" industry we remain prepared to work with the GAC and GAC members to appropriately identify all relevant bodies to develop a strategy to maintain a working relationship with them, as well as to explore to include additional safeguards where appropriate in consultation with ICANN and the GAC.

5. Registrants must be required by the registry operators to notify to them a single point of contact which must be kept up-to-date, for the notification of complaints or reports of registration abuse, as well as the contact details of the relevant regulatory, or industry self-regulatory, bodies in their main place of business.

We are supportive of the conceptual direction of this advice to be able to connect with registrants in a timely fashion. At the same time, we also understand that within the current ICANN gTLD Registry-Registrar framework, the Registry should rely on the Sponsoring Registrar to connect with registrants. Many Registrars feel that it is inappropriate for the Registry to directly contacting the registrant.

Nevertheless, in balancing the above considerations, it is possible to setup an "Operations and Notifications Contact" (for example, this was approach was successfully implemented to address similar conditions during the original .ASIA ASCII launch), which Registrars and/or registrants may select to nominate, with default being either the Registrar contact or the Admin Contact for the registrant.

We are prepared to explore to include additional safeguards where appropriate in consultation with ICANN and the GAC.

The GAC further advises the Board: 1. In addition, some of the above strings may require further targeted safeguards, to address specific risks, and to bring registry policies in line with arrangements in place offline. In particular, a limited subset of the above strings are associated with market sectors which have clear and/or regulated entry requirements (such as: financial, gambling, professional services, environmental, health and fitness, corporate identifiers, and charity) in multiple jurisdictions, and the additional safeguards below should apply to some of the strings in those sectors: 6. At the time of registration, the registry operator must verify and validate the registrants' authorisations, charters, licenses and/or other related credentials for participation in that sector.

Credentials of registrants will be checked with the Registrant pre-verification and authentication process as part of the Abuse prevention and mitigation mechanisms (#28):

Registrant pre-verification and authentication

One of the systems that could be used for validity and identity authentication is VAULT (Validation and Authentication Universal Lookup). It utilizes information obtained from a series of trusted data sources with access to billions of records containing data about individuals for the purpose of providing independent age and id verification as well as the ability to incorporate additional public or private data sources as required.

At present it has the following: US Residential Coverage - 90% of Adult Population and also International Coverage - Varies from Country to Country with a minimum of 80% coverage (24 countries, mostly European).

Various verification elements can be used. Examples might include applicant data such as name, address, phone, etc. Multiple methods could be used for verification include integrated solutions utilizing API (XML Application Programming Interface) or sending batches of requests.

• Verification and Authentication requirements would be based on TLD operator requirements or specific criteria.
• Based on required WHOIS Data; registrant contact details (name, address, phone)
• If address/ZIP can be validated by VAULT, the validation process can continue (North America +25 International countries)
• If in-line processing and registration and EPP/API call would go to the verification clearinghouse and return up to 4 challenge questions.
• If two-step registration is required, then registrants would get a link to complete the verification at a separate time. The link could be specific to a domain registration and pre-populated with data about the registrant.
• If WHOIS data is validated a token would be generated and could be given back to the registrar which registered the domain.
• WHOIS data would reflect the Validated Data or some subset, i.e., fields displayed could be first initial and last name, country of registrant and date validated. Other fields could be generic validation fields much like a "privacy service".
• A "Validation Icon" customized script would be sent to the registrants email address. This could be displayed on the website and would be dynamically generated to avoid unauthorized use of the Icon. When clicked on the Icon would show limited WHOIS details i.e. Registrant: jdoe, Country: USA, Date Validated: March 29, 2011, as well as legal disclaimers.
• Validation would be annually renewed, and validation date displayed in the WHOIS.

Eligibility of Registrants are verified and subject to challenge during startup phases including Sunrise. We plan to gradually open up the namespace for general registration while continuing requiring registrants to abide by registration policies. Pre-verification processes will be simplified gradually with increased post-registration enforcement supported by anti-abuse measures as described above and in our application #28 Abuse Prevention and Mitigation.

We are prepared to explore to include additional safeguards and moderate the pre-verification processes where appropriate in consultation with ICANN and the GAC.

7. In case of doubt with regard to the authenticity of licenses or credentials, Registry Operators should consult with relevant national supervisory authorities, or their equivalents.

We are supportive of and fully prepared to be compliant with the advice.

As mentioned in 4. above, we are prepared to work with the GAC and GAC members to identify relevant authorities, organizations and bodies to refer to for various processes, including to assess authenticity and consider appropriateness of activities for domain registrations.

We are prepared to explore to include additional safeguards and to identify and work closely with other relevant authorities where appropriate in consultation with ICANN and the GAC.

8. The registry operator must conduct periodic post-registration checks to ensure registrants' validity and compliance with the above requirements in order to ensure they continue to conform to appropriate regulations and licensing requirements and generally conduct their activities in the interests of the consumers they serve.

We are supportive of, fully prepared to be, and believe that our proposal is already compliant with the advice.

That being said, we again emphasize that within the current ICANN gTLD Registry-Registrar framework, the Registry should rely on the Sponsoring Registrar to connect with registrants. Many Registrars feel that it is inappropriate for the Registry to directly contacting the registrant. Therefore, while we will proactively check compliance, in terms of enforcement, we intend to work closely with Registrars to administer corrective measures.

Furthermore, we will develop and implement processes for community, industry and/or public reporting of compliancy issues. These have been included in our responses to #28 and #29 of our application.

We are prepared to explore to include additional safeguards and processes where appropriate in consultation with ICANN and the GAC.