

## 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 Communiqué](#) 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	fTLD Registry Services, LLC
Application ID	1-1035-75923
Applied for TLD (string)	.insurance

### Response:

fTLD Registry Services, LLC (fTLD), the community-based applicant for the .bank and .insurance generic Top-Level Domains (gTLDs), is providing this response to the recently issued Governmental Advisory Committee (GAC) Advice on New gTLDs as required by Section 3.1 of the Applicant Guidebook. fTLD acknowledges the significant undertaking that was before GAC for it to meet its commitment to provide Advice by 13 April 2013, and we appreciate the care and level of detail that it provided in its [Beijing Communiqué](#).

fTLD is owned, operated and governed by members of the financial services community and is committed to operating financial gTLDs fairly, transparently and in a manner that serves and protects the community and the consumers/Internet users it serves. It was at the community’s urging that community-based applications for .bank and .insurance should be filed to protect the community and it is for that reason that fTLD was formed. As such, we are pleased to see the GAC’s recognition and affirmation of the value of community-based applications in its statement, “that in those cases where a community, which is clearly impacted by a set of new gTLD applications in contention, has expressed a collective and clear opinion on those applications, such opinion should be duly taken into account, together with all other relevant information.”

Regarding GAC’s Advice on safeguards, fTLD supports those identified for all new gTLDs and the additional safeguards for gTLDs that represent regulated markets. In fact, most of the safeguards are indicative of activities that fTLD anticipated it would need to implement given the public interest implications of .bank and .insurance. This is why the American Bankers Association and The Financial Services Roundtable advocated on behalf of the community for additional safeguards and fTLD ultimately included measures to address many of the safeguards that in the end became GAC Advice for the .bank and .insurance applications. Following the public comment period on, and the ICANN Board’s consideration of GAC Advice,

## GAC Advice Response Form for Applicants



New Generic Top-Level  
**Domains**

fTLD is committed to implementing approved safeguards including those that will require some modifications to fTLD's procedures and/or systems (see Annex).

If fTLD has been approved to operate new gTLDs, it will be bound by Section 2.19, Operations of Registry Operator to TLD Community, and Specification 12, Community Registration Policies, of its Registry Agreement with ICANN. It is through these contractual provisions that fTLD will fulfill on its commitments to the community including those that were included in its applications and be subject to ICANN's compliance activities including, but not limited to, the [Registry Restrictions Dispute Resolution Procedure](#).

fTLD continues to believe that the introduction of new gTLDs has the potential to enhance consumer choice, promote competition and to foster innovation in the domain name system. We also firmly believe that in the cases of gTLDs that have unique trust implications, including those identified by the GAC, they must only be awarded to a trusted member of the community that will operate them with strict registration restrictions and in a manner that puts the public interest above the maximization of revenue.

Respectfully,

A handwritten signature in blue ink that reads "Craig S. Schwartz".

Craig S. Schwartz  
Director  
fTLD Registry Services, LLC

# GAC Advice Response Form for Applicants



New Generic Top-Level  
**Domains**

## Annex

GAC ADVICE	FTLD RESPONSE
<p>In those cases where a community, which is clearly impacted by a set of new gTLD applications in contention, has expressed a collective and clear opinion on those applications, such opinion should be duly taken into account, together with all other relevant information.</p>	<p>fTLD agrees and notes that our applications have extensive endorsements from the community. See list of current endorsers at <a href="http://www.ftld.com/endorsers.html">http://www.ftld.com/endorsers.html</a>.</p>
<p>A. Safeguards Applicable to all New gTLDs</p>	
<p>1. WHOIS (registration information) and checks: should be conducted on a statistically significant basis at least twice a year.</p>	<p>fTLD agrees and would like to highlight that our applications go above and beyond this requirement including a commitment to verify all WHOIS records at least semi-annually in compliance with the Enhanced Security Standards provided to ICANN on 11 December 2011 (see <a href="http://www.icann.org/en/correspondence/aba-bits-to-beckstrom-crocker-20dec11-en.pdf">http://www.icann.org/en/correspondence/aba-bits-to-beckstrom-crocker-20dec11-en.pdf</a>). See Standard #23.</p>
<p>2. Mitigating abusive behavior: acceptable use and/or abuse policy to be defined.</p>	<p>fTLD agrees and notes that our applications are in compliance with requirements #3 and #16 in the above referenced Enhanced Security Standards.</p>
<p>3. Security checks: regular checks should be done to assess if domains are being used to perpetrate security threats and registries should suspend domains if registrar won't.</p>	<p>fTLD agrees and has affirmatively addressed this point in our response to question 20(e).</p>
<p>4. Documentation: statistical reports that provide the number of inaccurate WHOIS records or security threats should be maintained and provided to ICANN upon request.</p>	<p>fTLD commits to making this information available to ICANN at their request based upon the information in items A1 and A3 that will be collected in accordance with representations made in our applications.</p>
<p>5. Making and handling complaints: there should be a mechanism for making complaints to the registry operator about inaccurate WHOIS information and/or domains being used for malicious activity or perpetuating security risks.</p>	<p>fTLD agrees and will modify the ticketing system identified in our response to Question 28 to include inaccurate WHOIS.</p>
<p>6. Consequences: there should be real and immediate consequences for providing false WHOIS information and/or if the domain is being used in breach of applicable law.</p>	<p>fTLD agrees and has set forth in our response to Question 28 fTLD's policies and procedures for domain names used in violation of the acceptable use/abuse policies.</p>
<p>B. Safeguards for New gTLDs Linked to Regulated or Professional Sectors</p>	
<p>1. Registry acceptable use policy must require registrants to 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</p>	<p>fTLD agrees and in responses to Questions 20(e) and 28 prohibit use of the domain for any purposes prohibited by the laws of the jurisdiction(s) in which the registrant does business and further lists examples of prohibited activities.</p>



## GAC Advice Response Form for Applicants

farming, disclosure of data, and financial disclosures.	
2. Registry operators will require registrars at the time of registration to notify registrants of the acceptable use policy.	fTLD agrees and notes that our applications are in compliance with requirement #19 in the above referenced Enhanced Security Standards.
3. Registry Operators will require 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.	fTLD agrees and this requirement will be part of the registration agreement registrants sign with their registrars.
4. Establish a working relationship with the relevant regulatory, or industry self-regulatory, body including developing a strategy to mitigate as much as possible the risks of fraudulent, and other illegal, activities.	fTLD agrees and has already begun this effort. This activity is anticipated as it relates to fTLD's ability to verify registrants. fTLD may however be limited by the relevant regulatory or industry self-regulatory bodies voluntary cooperation with fTLD.
5. Registrants must be required by the registry operator to provide a single point-of-contact 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.	fTLD agrees in principle and Enhanced Security Standards #8 and #9 in part address this for registry operators and registrars and this could be expanded to registrants. fTLD commits to work with relevant regulatory or industry self-regulatory bodies identified above to collect the relevant contact details to address the concerns of the GAC.
C. Additional Safeguards for New gTLDs Associated with Market Sectors that have clear and/or Regulated Entry Requirements	
1. At the time of registration the registry operator must verify and validate the registrants' authorizations, charters, licenses and/or other credentials for participation.	fTLD agrees and Enhanced Security Standard #22 incorporated into our applications addresses this item.
2. In case of doubt with regard to authenticity of licenses or credentials, registry operator should consult with relevant national supervisory authorities, or other equivalents.	fTLD agrees. This item is explicitly linked to safeguards C1 and implicitly linked to B4.
3. Registry operator must conduct periodic, post-registration checks 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.	fTLD agrees and has proactively responded to this issue in response to Question 20(e) concerning auditing of domain names to ensure compliance with acceptable use/abuse policies.
4. The registry operator should administer access in these kinds of registries in a transparent way that does not give an undue preference to any registrars or registrants, including itself, and shall not subject registrars or registrants to an undue disadvantage.	fTLD affirms its commitment that its gTLDs will be operated fairly, transparently, without undue preference and in the best interest of the community.