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	DotHealth LLC
Application ID	1-1684-6394
Applied for TLD (string)	health

Response:

May 10, 2013

Response to the Government Advisory Committee (GAC) Advice Within the Beijing Communiqué issued on April 11, 2013

DotHealth, LLC applied to ICANN (Application ID: 1-1684-6394) to operate the .health new generic top level domain (TLD) Registry. We thank ICANN for the opportunity to submit these comments in response to the GAC Advice on safeguards applicable to new generic top-level domain names (gTLDs).

General Comments

The GAC considers that Safeguards should apply to broad categories of strings...in the current or future rounds, in all languages applied for. While the GAC's intent to divide strings into categories is a noble effort, we believe that this is a difficult, if not impossible task to undertake in a fair, consistent, meaningful and transparent manner. Strings have multiple meanings, different applications to different users in different markets, etc. They do not easily fall into categories and therefore we are opposed to the categorization of strings.

The GAC with its very wide set of advice appears to contradict many of the principles and requirements set forth by ICANN in the Applicant Guidebook ("AGB") for the gTLD program. If the board were to accept all the GAC advice this would materially impact applicants businesses including revenue and cost projections. The principles and rules developed by ICANN were developed during years of bottoms up consultation within the community and should be adhered to unless there is a compelling reason to deviate.

Applicants such as ourselves who have already identified the relevant issues for health and included a high degree of safeguards to protect health stakeholders ironically do not benefit from the GACs advice. Those applicants that have not taken similar steps apparently are now being given the opportunity to rewrite their applications in an attempt to gain competitive advantage.

Furthermore, requiring the implementation of these Safeguards as broadly proposed would go against the GAC's own established Principles Regarding New gTLDs, as published in March 2007 which included this principle among others:

2.5. The evaluation and selection procedure for new gTLD registries should respect the principles of fairness, transparency, and non-discrimination. All applicants for a new gTLD registry should therefore be evaluated against transparent and predictable criteria, fully available to the applicants prior to the initiation of the process. Normally, therefore, no subsequent additional selection criteria should be used in the process.

In addition, the lack of specificity provided by the GAC in its advice implies that any proposed safeguard by an applicant – regardless of the level of impact and benefit of the safeguard, would all be judged equally by the GAC since no criteria or specificity has been offered.
The GAC advice appears to written based on an incorrect assumption that the gTLD's applied for are the only gTLD's that exist around the world. This ignores the fact that today almost 250 TLD's are currently in operation with varying degrees of safeguards – most of which fall far short of the safeguards proposed by applicants in this gTLD application round. The implications of this fact, given that existing TLD's would not be subject to the vast majority of GAC advice, would set up a puzzling and inconsistent situation for worldwide Internet users. This is primarily because any TLD may be accessed by any user, in any geographic location.

Those individuals or entities that wish to circumvent newly established requirements could easily do so without constraint -- a fundamental reason why enforcing adherence to laws and regulations is not an appropriate role for a gTLD registry operator. Federal, state, and local authorities in combination with the appropriate regulatory agents in any given jurisdiction, industry, or market segment are empowered and expected to enforce regulations with the cooperation of the registry operator. The GAC advice turns this model on its head and we believe it represent an unworkable proposition.

Although the GACs intentions are laudable, similar efforts in the past by governments to hold telecommunications providers, search engines, network operators, cable and satellite television providers, etc. accountable for the activities and content produced and presented by others on such networks have generally been a failure.

Safeguards Applicable to all New gTLDs

The GAC has advised that six general Safeguards (#1-6) should apply to all new gTLDs and shall be subject to contractual oversight: 1) WHOIS verification and checks; 2) Mitigating abusive activities; 3) Security checks; 4) Documentation (of WHOIS records and other reports); 5) Making and Handling Complaints; and 6) Consequences (for registrants who violated policies).

DotHealth wishes to highlight the fact that in its application to ICANN for the .health TLD, DotHealth addresses each of the safeguards in some form, as standard policies or procedures, some of which we have contracted for through our Registry Service Provider, Neustar.
In addition, DotHealth filed public interest commitments (PICs) for its application for .health, committing to the implementation of these types of safeguards.

As a prospective registry operator for the .health TLD, we have developed our own methodologies within ICANN policy guidelines and best practices for conducting security checks, maintaining statistical reports and addressing violations of their terms of service. Although we have committed to implementing these Safeguards, what we've proposed is what we believe is most appropriate and necessary for the stakeholders and use case for the .health gTLD. The GAC is not is a position to dictate the specific processes or methodologies. Registry operators should simply consult best practice and ICANN guidelines in order to implement the particular solutions that fit within the Registry's business model.

Safeguards 1-6

To further ensure the GAC has full clarity on our approaches for meeting its suggested requirements and commitments as they relate to the general safeguards as proposed, the following feedback and information have been provided:

-Recommended Safeguard #1: WHOIS Verification and Checks

The New gTLD Policy contains a variety of new, mandatory rights protection mechanisms for trademark owners. The goal of improved WHOIS accuracy in the new gTLD context has been the subject of intensive discussions and negotiations among registrars, the GAC, law enforcement, and the community for several years. Inspired, in part, by GAC demands and threats, registrars have spent countless hours over the last 18 + months working with ICANN and law enforcement to craft a Registrar Accreditation Agreement (RAA) for the New gTLD program. The draft agreement, which is now posted for public comment, addresses a long list of LEA and GAC requests and saddles registrars with significant new obligations related to verification and validation of WHOIS data. In addition, the new RAA already requires registrars to create audit trails so that ICANN can evaluate and hold registrars accountable for any failure to act on reports of missing, inaccurate, or incomplete WHOIS data.

Additionally, as specified our application, DotHealth, LLC committed to regularly monitor registration data for accuracy and completeness, and establish policies and procedures to address domain names with inaccurate or incomplete WHOIS data in a manner consistent with the GAC Advice.

As a reminder, as described in our application response and answer to Question 28 (Abuse Prevention and Mitigation), and reinforced in our PIC's of March 5, 2013:

- DotHealth shall on its own initiative, no less than twice per year, perform a manual review of a random sampling of .health domain names to test the accuracy of the WHOIS information. DotHealth will examine the WHOIS data for prima facie evidence of inaccuracies. In the event that such evidence exists, it shall be forwarded to the sponsoring Registrar, who shall be required to address those complaints with their registrants.

- Thirty days after forwarding the complaint to the registrar, the Applicant will examine the current WHOIS data for names that were alleged to be inaccurate to determine if the information was corrected, the domain name was deleted, or there was some other disposition. If the Registrar has failed to take any action, or it is clear that the Registrant was either unwilling or unable to correct the inaccuracies, DotHealth shall reserve the right to suspend the applicable domain name(s) until such time as the Registrant is able to cure the deficiencies.

-GAC Recommended Safeguard #2: Mitigating Abusive Activity

An obligation to comply with applicable law is generally an imputed term in all agreements. Presumably, the GAC has made this recommendation because it intends to obligate registries to play a role in enforcing the terms and conditions of an agreement (the registrar-registrant agreement) to which it is not even a party. But participants in the RAA negotiations – including law enforcement – have acknowledged that registrars themselves will often lack both the facts and the legal expertise required to determine (a) what law applies to a particular registrant's conduct and (b) whether specific conduct is prohibited under the law that does apply. That is precisely why ICANN has adopted Consensus Policies such as the UDRP, Rapid Suspension, etc., which create expert bodies to evaluate registrant conduct in relationship to those policies (as opposed to the law of a particular sovereign). That is also why the rights protections mechanisms in the New gTLD Policy, as reflected in the Applicant Guidebook, do not impose this kind of operational responsibility on new gTLD registry operators. Indeed, the new RAA, which is extremely responsive to law enforcement recommendations, takes a different approach that reflects the appropriate role of registrars in supporting law enforcement activities by requiring dedicated points of contact, mandating specific data collection and retention practices, etc. But even that document - which has been the object of community discussion for nearly two years now - does not propose to deputize contracted parties to serve as extensions of law enforcement or the judicial system.

DotHealth re-affirms those commitments made in our application to ICANN for the .health TLD to 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 also wish to reinforce that throughout our application to ICANN for the .health TLD, we have readily acknowledged that abusive practices and malicious behaviors including email spam, search-engine optimization, social network abuse, typo-squatting, and others are increasingly commonplace in the current landscape of online health, and potentially pose harm to consumers and other stakeholders in global health. Notably, the safeguards DotHealth has proposed for the .health TLD have been specifically identified to address these concerns, and which far surpass those that exist today in other current top level domains.

As described in our application response and answer to Question 28 (Abuse Prevention and Mitigation):

DotHealth will adopt and enforce compliance with an Acceptable Use Policy that clearly defines the types of activities that will not be permitted for users of the .health TLD. Each ICANN-

Accredited Registrar must agree to pass through the Acceptable Use Policy to its Resellers (if applicable) and ultimately to all .health registrants.

The following activities are subject to compliance with this policy:

- Phishing: the attempt to acquire personally identifiable information by masquerading as a website other than .health.

- Pharming: the redirection of Internet users to websites other than those the user intends to visit, usually through unauthorized changes to the Hosts file on a victim's computer or DNS records in DNS servers.

- Dissemination of Malware: the intentional creation and distribution of "malicious" software designed to infiltrate a computer system without the owner's consent, including, without limitation, computer viruses, worms, key loggers, and Trojans.

- Fast Flux Hosting: a technique used to shelter Phishing, Pharming and Malware sites and networks from detection and to frustrate methods employed to defend against such practices, whereby the IP address associated with fraudulent websites are changed rapidly so as to make the true location of the sites difficult to find.

- Botnetting: the development and use of a command, agent, motor, service, or software which is implemented: (1) to remotely control the computer or computer system of an Internet user without their knowledge or consent, (2) to generate direct denial of service (DDOS) attacks.

- Malicious Hacking: the attempt to gain unauthorized access (or exceed the level of authorized access) to a computer, information system, user account or profile, database, or security system.

- Child Pornography: the storage, publication, display and/or dissemination of pornographic materials depicting individuals under the age of majority in the relevant jurisdiction.

- Illicit Promotion or Sale of Harmful Substances: the illicit promotion or sale of prescription drugs, controlled substances, tainted dietary supplements, ingredients for psychoactive highs, and others which are have been validated by regulatory authorities as safety concerns.

This Acceptable Use Policy gives the .health registry the ability to quickly lock, cancel, transfer or take ownership of any .health domain name, either temporarily or permanently, if the domain name is being used in a manner that appears to threaten the stability, integrity or security of the Registry, or any of its registrar partners – and/or that may put the safety and security of any registrant or user at risk.

In the interest of protecting rightsholders and intellectual property stakeholders, numerous operating procedures, safeguards and policies have been identified and orchestrated in conjunction with our proposed efforts to operate the .health TLD registry. These are fully detailed and explained in our application to ICANN, and reinforced in our PIC's of March 5, 2013.

We wish to further note that ICANN has a web-based process for complaints about non-responsive registrars. ICANN and registrars continue to attempt to resolve significant issues related to frivolous and harassing complaints, and it makes little sense to create two different systems. To the extent any registry involvement is necessary for the .health TLD , it should be sufficient for DotHealth to provide a link to the ICANN page at: http://reports.internic.net/cgi/registrars/problem-report.cgi.

-GAC Recommended Safeguard #3: Security Checks

This Advice appears to be encompassed in the GAC's Advice regarding abuse mitigation, above. It is addressed in the 2013 RAA through the new obligation that registrars provide 24/7 abuse contact information for use by relevant law enforcement, consumer protection authorities, etc., to report potentially illegal activities, and the requirement that such reports are reviewed and responded to within a specific time period. ICANN has the authority to audit registrar compliance with this obligation, and has a variety of enhanced enforcement tools to address non-compliance. Despite the clear focus on this issue in the context of the 2013 RAA, the GAC's Advice creates a completely new, unanticipated cost – and associated legal liability to registrars and registrants – on new gTLD applicants. We feel it is inappropriate to use the String Objection procedures in the New gTLD Applicant Guidebook to create significant new policy applicable to all TLDs.

DotHealth re-affirms its commitments as described in our application to ensuring that those domain names associated with abuse or malicious conduct (including phishing, pharming, botnets, etc.) are dealt with in a timely and decisive manner. As reinforced in our PIC's of March 5, 2013

- Once a complaint is received from a trusted source, a third-party, or detected by the Registry, the Registry will use commercially reasonable efforts to verify the information in the complaint.

- If that information can be verified to the best of the ability of the Registry, the sponsoring registrar will be notified and be given 12 hours to investigate the activity and either take down the domain name by placing the domain name on hold, deleting the domain name in its entirety or remedying the abusive practices.

- If the registrar has not taken the requested action after the 12-hour period (i.e., is unresponsive to the request or refuses to take action), the Registry will place the domain on "ServerHold." Although this action removes the domain name from the .health TLD zone, the domain name record still appears in the .health TLD WHOIS database so that the name and entities can be investigated by law enforcement should they desire to get involved.

-GAC Recommended Safeguard #4: Documentation

ICANN has a web-based process for complaints about non-responsive registrars. ICANN and registrars continue to attempt to resolve significant issues related to frivolous and harassing complaints. Therefore, DotHealth believes it makes little sense to create two different systems. To the extent any .health TLD registry involvement is necessary, we feel it should be sufficient for DotHealth to provide a link from our registry web site to the ICANN page at: http://reports.internic.net/cgi/registrars/problem-report.cgi

-GAC Recommended Safeguard #5: Making and Handling Complaints

DotHealth re-affirms its commitments as described in our application for the .health TLD to these recommended safeguards. As described in our application response and answer to Question 28 (Abuse Prevention and Mitigation):

DotHealth will establish and publish on its website a single abuse point of contact responsible for addressing inquiries from law enforcement and the public related to malicious and abusive conduct. DotHealth will also provide such information to ICANN prior to the delegation of any domain names in the .health TLD. This information shall consist of, at a minimum, a valid e-mail address dedicated solely to the handling of malicious conduct complaints, and a telephone number and mailing address for the primary contact. We will ensure that this information will be kept accurate and up to date and will be provided to ICANN if and when changes are made. In addition, with respect to inquiries from ICANN-Accredited registrars, our back-end registry service provider, Neustar, shall provide an additional point of contact, as it does today, handling requests by registrars related to abusive domain name practices.

In the event that we receive a complaint that a .health domain name is being used in a manner that appears to threaten the stability, integrity or security of the Registry, or any of its registrar partners – and/or that may put the safety and security of any registrant or user at risk, DotHealth shall take preventive measures to avoid any such criminal or security threats which may be triggered through a variety of channels, including, among other things, private complaint, public alert, government or enforcement agency outreach, and the ongoing monitoring by the Registry or its partners. In all cases, the Registry or its designees will alert Registry's registrar partners about any identified threats, and will work closely with them to bring offending sites into compliance.

For the .health TLD, DotHealth's back-end registry provider and partner, Neustar, will target verified abusive domain names and remove them within 12 hours regardless of whether or not there is cooperation from the domain name registrar. In the event a domain name is being used to threaten the stability and security of the .health TLD, including and not limited to suspected privacy or security breaches, or in a case a domain is part of a real-time investigation by law enforcement or security researchers, its resolution will be disabled completely within the DNS master zone file that enables such resolution. Removing the domain name from the zone has the effect of shutting down all activity associated with the domain name, including the use of all websites and e-mail addresses mapping to the domain name in question.

-GAC Recommended Safeguard #6: Consequences

The WHOIS issues are addressed directly in the new 2013 RAA, which requires registrars to verify WHOIS information in response to reports of inaccuracy and, if they unable to do so, to suspend such registrations. It does not make sense to create potentially conflicting enforcement models. Moreover, this approach creates potentially significant liability to registrants – with whom registries do not have direct relationships in most cases.

Likewise, the new RAA requires registrars to provide Abuse Contact information and imposes a duty to investigate reports of registrant abuse. Registrars must provide monitored points of contact to receive reports of illegal activity by law enforcement, consumer protection, quasi-governmental or other similar authorities.

ICANN has a web-based process for complaints about non-responsive registrars. ICANN and registrars continue to attempt to resolve significant issues related to frivolous and harassing complaints, and it makes little sense to create two different systems. To the extent any registry involvement is necessary on the part of DotHealth as the registry operator for the .health TLD, we believe it should be sufficient for us to provide a link to the ICANN page at:
http://reports.internic.net/cgi/registrars/problem-report.cgi

Category 1 Safeguards

In addition to the six general Safeguards applicable to all new gTLDs, the GAC has advised that five additional "Category 1" safeguards be implemented for:
"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:"

DotHealth believes the GAC Advice pertaining to Category 1 Strings is inconsistent and cannot be implemented. This sweeping statement is overbroad and ignores entirely the important issue of context. The GAC Advice provides no principled basis for understanding why some strings are included and others are not. For example, as specified by the GAC, the "Health and Fitness" category includes:

- .care, BUT NOT .help
- .fit BUT NOT .yoga or .coach
- .clinic BUT NOT .salon

First, we firmly believe that ALL strings should operate in a way that is consistent with applicable laws. There is no logical reason for a limited number of strings to be singled out.

Second, the term "linked" is an insufficient criteria to judge which gTLD's should be subject to these Category 1 safeguards. To what degree does the linkage need to be? What type of linkage? What if the linkage isn't consistent across various geographic jurisdictions? What defines a linkage? How would a registry operator know which linkages the GAC is referring to? What if there is a difference of opinion amongst entities involved in a specific area as to policy? What if there are so many sectors covered by the string that it is impossible to identify all the linkages?

Third, we believe that ALL TLDs invoke some level of implied trust. The question is - what level? Since trust is a perceived attribute on the part of an individual, not necessarily based on the string or meaning of the string itself, but rather on how the registry operates and what actions it does or does not take over a period of time to ensure this trust. Levels of trust also vary over time. The key point is that all TLD's should therefore be covered under GAC advice for category 1 – not just a subset of TLD's. There is also no way of identifying and quantifying "levels of risk associated with consumer harm”. We are unaware of any objective source that can be turned to in order to identify these levels. Furthermore, there is no basis for assuming that risk to consumers is string specific. Again, the risk is related to the actual behavior of both registrants and consumers on a particular website.

Fourth, not only is it unclear which sectors in relation to each string are covered under the advice, but the GAC states safeguards “should apply to strings that are related to these sectors”. Related in what way? To what extent? There is no objective way to interpret the word “related” and the GAC has not attempted to clarify its intent. This produces an unworkable situation for registries.

We wish to reinforce that our goal, and actually a fundamental part of our proposed business model, is to make the Internet a safer, reliable and genuinely trustworthy resource for all stakeholders in health. If we are not successful doing this, we don’t expect to succeed.
We respectfully provide the following feedback in specific response to those safeguards that the GAC has recommended for Category 1 (page 8-9 of the GAC Beijing Communiqué):

GAC Suggested Safeguard #1 (Category 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.

As discussed above, registrants in .health are inherently obligated to comply with applicable laws relating to privacy, data collection, consumer protection, fair lending, debt collection, etc. The proposition that registrants are liable for their conduct under applicable law is not contested. The GAC Advice, however, would impose liability on registry operators with respect to registrant conduct, and require registry operators to identify the law applicable to any particular registrant, and to evaluate the conduct of a registrant against such law. While registries and registrars are obligated to cooperate with and assist appropriate law enforcement agencies in accordance with applicable due process requirements, “outsourcing” law enforcement to the private sector, particularly in a multi-jurisdictional global environment raises significant policy, due process, and business concerns that must be addressed.

Within the many sectors, segments, and interests that have “health” contexts, there is a lack of common definition, levels of adoption, and applicable laws for the privacy, collection, protection, disclosure or security of health or financial information. Such laws or guidelines are established by a variety of law enforcement, regulatory agencies and industry expert bodies in any given country or jurisdiction. In many cases, these complex issues are under discussion and debate by working groups with representation across segments, and represent some of the most challenging issues to gain consensus about. It is simply not, and should not be, the role or responsibility of a registry operator - that by definition does not see 100% of the activity related to any sector, to be asked to assume responsibility or liability, or be accountable for enforcement.

GAC Suggested Safeguard #2 (Category 1):

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

As previously described herein, DotHealth will adopt and enforce registrar (including re-sellers) and registrant compliance with an Acceptable Use Policy (AUP) that clearly defines the types of activities that will not be permitted for all users of the .health TLD. Indeed, all registrants will be notified of the AUP at the time of registration and will be obligated to accept the terms and conditions set forth in the Acceptable Use Policy.

-GAC Suggested Safeguard #3 (Category 1):

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.

Privacy and data security requirements are established by national and local law, and vary dramatically from country to country. It is entirely reasonable to expect registry operators to handle data they collect and maintain to comply with applicable data privacy and security laws. It is also reasonable to require registrants to be transparent about their data collection and processing practices, but in most situations it is unreasonable to expect registry operators to pass judgment on what law applies to a registrant's conduct and whether or not that conduct is consistent with applicable law.

Although the GAC's goals and objectives for establishing increased levels of privacy and security for sensitive health and/or financial information are laudable, with respect to these safeguards, the GAC has failed to provide any specifics that would help to determine whether or not any registry operator could conceivably meet such requirements.

The GAC's broadly suggesting safeguards for any health-related TLD string (including .health) on the basis of "applicable laws" suggests it has failed to appropriately consider the many complex issues which are associated with health information privacy or security, among others. For example, the GAC has not clearly defined what "sensitive health and financial data" means, or what "services" the advice actually refers to, or what "security measures" are actually required. Additionally, the suggested safeguards fail to provide any criteria which would be used to determine how these might be considered commensurate with the offering of those services" and how these may or may not apply to various types of registrants that are considered for the .health TLD. If meant to address those registrants that collect or exchange sensitive health or financial information, as previously noted, applicable laws and security requirements will and should govern registrant activities.

GAC Suggested Safeguard #4 (Category 1):

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.

Successfully mitigating risks of fraudulent, and other illegal, activities may or may not require a working relationship with regulatory bodies. The GAC advice assumes that the only way to do this is by establishing such working relationship.

DotHealth LLC believes it is important to mitigate fraud and illegal activities. To the extent that there are identifiable and relevant regulatory bodies that are open and willing to participate with the Registry operator, it should be encouraged, but it should not be a mandatory requirement. There are enforcement issues and many complications that arise. Who does one work with when a string like health has multiple meanings in multiple segments and therefore multiple regulatory bodies? What happens if the regulatory body is not cooperative? What if there are competing regulatory bodies with opposite agendas? Who do you work with when you couldn't possibly satisfy both bodies? For these reasons and many others, we feel this Safeguard is impractical to require. Further what exactly does a "working relationship" mean? No criteria have been offered to determine the level and outcome of such a relationship.

DotHealth has indeed formed working relationships with many respected industry players, including Neustar, Inc. and LegitScript, LLC. DotHealth has received affirmations of support from the National Association of Boards of Pharmacy (NABP), the World Federation of Chiropractic, the Inter-American College of Physicians and Surgeons, the Association of Black Cardiologists, and the Regulatory Harmonization Institute. However, there are literally thousands of organizations representing various stakeholder interests and we believe the registry itself should be able to determine which bodies are most "relevant" to work with. There are no objective criteria suggested by the GAC to determine the level of "relevance".

As an example of how we are addressing the GAC's proposed safeguards, DotHeath's partner and back-end registry services provider Neustar Inc. has established and maintains on-going cooperation with law enforcement agencies and well-known security organizations throughout the world including the Anti-Phishing Working Group, NSP-SEC, the Registration Infrastructure Safety Group, and others. Aside from these organizations, Neustar also actively participates in privately run security associations whose basis of trust and anonymity makes it much easier to obtain information regarding abusive DNS activity, all of which will be of key input to the operation of the .health TLD.

Neustar's commitment to consumer protection in the health arena is further reflected in its service as a founding board member of The Center for Safe Internet Pharmacies (CSIP), a non-profit organization chartered in 2011 to address the growing problem of internet sales of illegitimate pharmaceutical products. CSIP's membership includes the world's leading Internet and e-commerce companies, domain name registrars, search engines, and financial services providers.

Another relevant example is our exclusive partnership with LegitScript for the .health TLD which will help us maintain .health as a trustworthy environment by monitoring the TLD on an enterprise basis for any unsafe and illegal activity involving the distribution of prescription drugs and controlled substances, as well as other illegal or unsafe products. Such a partnership represents the first time that an entire registry will be protected in this way from rogue online pharmacies and illicit advertisements for harmful substances, not only in the US, but also around the entire world.

As the world's leading provider of online surveillance and monitoring solutions, LegitScript currently works with numerous governments and government agencies, including the U.S. Food and Drug Administration, INTERPOL, the Irish Medicines Board, and the National Association of Boards of Pharmacies in the US to develop international standards that are applied. LegitScript also provides surveillance and investigative reporting services leading search engines to ensure that advertising on these search engines is for legitimate products from legitimate companies.

GAC Suggested Safeguard #5 (Category 1):
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.

The substantive requirements of this GAC request has been fully incorporated into the 2013 RAA, which requires registrars to maintain a 24/7 monitored, single point of contact to receive abuse reports from designated law enforcement, consumer protection, and quasi-governmental or similar authorities, to publish their complaint processing policies and procedures, and to maintain auditable records of their responses to such complaints. As described in our application to ICANN for the .health TLD and answers to Question 28 (Abuse Prevention and Mitigation):

DotHealth will establish and publish on its website a single abuse point of contact responsible for addressing inquiries from law enforcement and the public related to malicious and abusive conduct. DotHealth will also provide such information to ICANN prior to the delegation of any domain names in the .health TLD. This information shall consist of, at a minimum, a valid e-mail address dedicated solely to the handling of malicious conduct complaints, and a telephone number and mailing address for the primary contact. We will ensure that this information will be kept accurate and up to date and will be provided to ICANN if and when changes are made. In addition, with respect to inquiries from ICANN-Accredited registrars, our back-end registry service provider, Neustar, shall provide an additional point of contact, as it does today, handling requests by registrars related to abusive domain name practices.

Additional Category 1 Safeguards

The GAC Advice also notes that "some strings" may require further targeted safeguards to address specific risks and adds Safeguards No. 6, No. 7, and No. 8 to the five Category 1 Safeguards as described above.

DotHealth believes that the "Further Advice" and safeguards proposed by the GAC do not accomplish the GACs apparent goal of risk mitigation.

DotHealth believes these particular safeguards can only apply in a small number of specific cases. Particularly, to the extent an applicant has indicated that second level-domains in a particular TLD will be limited to licensed providers of product or services (which we are not), it would be appropriate to expect an applicant to propose policies designed to enforce such limitations. In the three additional safeguards above, however, the GAC is not giving advice related to applicant accountability. Instead it is creating general policy based on the overly broad and simplistic assertion a particular ecosystem and use of a particular string, relate solely to market sectors that have clear and/or regulated entry requirements. In practice this assumption does not translate to health.

Whether or not any of these Safeguards can be implemented in a practical manner is also very much in doubt. In principle, the entire concept of these Safeguards is fundamentally flawed in that these are criteria that are being created and introduced after the commencement of the initial evaluation process and subsequent even to the PIC process (which in itself was introduced long after the application window had closed). The development of this proposal is completely negates ICANN’s bottom-up, multi-stakeholder model. If the ICANN Board approved any one of these three safeguards, ICANN’s consensus driven policy making would be completely undermined.

Furthermore, we applied for this TLD under the assumption that we were applying for a generic TLD. These three Safeguards change the nature of the TLD we applied for from generic and widely available, to being “sponsored” TLDs, restricted only to those individuals who must prove their status or credentials entitling them to register domain names with certain extensions. This is not what the new gTLD program was intended for and the sponsored TLD rounds have long come and gone.

As a matter of feasibility, the implementation of such additional safeguards presumes that an authoritative and updated data set for each and every type of professional or business associated with identified with each and every entity or individual that comprises the addressable market of registrants would be readily available in electronic format in every country throughout the world. Additionally, this assumes such data is available for the purposes of licensing or use by TLD registry operators, registrars and others that are engaged in the domain name registration and renewal lifecycle.

However, the creation and maintenance of the tools and data sources would inevitably introduce development and licensing costs that weren't factored into a registry applicant's operational, technical and financial models that were prepared and submitted to ICANN. Furthermore, such safeguards might have a discriminatory effect on users in certain fields and on some developing nations whose governments do not have regulatory bodies or keep databases which a registry and/or a registrar could work with to verify certifications or credentials. The GAC Advice should not have the effect of putting developing countries at a disadvantage because they do not have infrastructures necessary to enable validation or verification.