VERISIGN

May 31, 2013

Internet Corporation for Assigned Names and Numbers
12025 Waterfront Drive, Suite 300
Los Angeles, California 90094-2536

Re: Reply Comments from Verisign Regarding the GAC's Safeguards Applicable to New gTLDs and Comments Related to Security and Stability

Dear ICANN:

As a long-time participant in, and supporter of, the multi-stakeholder model of Internet governance, Verisign acknowledges ICANN's Governmental Advisory Committee (GAC) for its recommendations to ICANN on the New gTLD Program, including its formal advice communicated in the April 11, 2013, Beijing Communiqué. We strongly encourage the ICANN Board to follow the multi-stakeholder model by engaging with the GAC, the new gTLD registry applicants, registrars and other members of the Internet community to carefully consider and discuss the GAC Advice to ensure it is given thorough consideration, implemented in the optimal manner consistent with the existing regulatory framework of rights and obligations of registries, registrars and registrants, and to determine the appropriate next steps to achieve these ends.

Verisign has been a registry operator for the largest top-level domains for more than 15 years and our experience with root operations is unparalleled. We have consistently led efforts to innovate registry and root operations and we take pride in our expertise. It is from this perspective, as a reliable and seasoned partner in the Internet ecosystem, that we submit constructive comments on the GAC's advice and how the ICANN Board could respond to that advice.

Verisign recognizes the GAC's vital role in bringing the perspectives of governments to our multi-stakeholder governance model. In this respect, the GAC's public policy advisory role necessarily continues into areas well beyond its April 11, 2013, advice on new gTLD strings. While the primary focus of our comments is on the GAC Safeguard Advice that applies to all new gTLDs, we have also included comments on specific security and stability concerns that have not yet been considered by the GAC, but must be addressed prior to any delegation.

Based on our extensive experience, Verisign has a unique perspective in the Internet community as to what is operationally critical to the continued security and stability of the DNS,

not just for new gTLDs, but for the entire DNS, including existing top-level domains. As such, we believe there are urgent security and stability concerns of critical importance to the GAC, and the governments it represents, that must be carefully assessed and remediated.

In our view, ICANN is struggling to balance two competing interests – the urgency felt by applicants to secure the earliest possible delegation of their new gTLDs against the need for responsible resolution of the security and stability concerns raised by the ICANN Board's own Stability and Security Advisory Committee (SSAC). We believe that, in light of this conflict, ICANN is at serious risk of assigning more weight to the former, at the expense of the latter. We urge the GAC to thoroughly review this issue and weigh in with the Board to ensure ICANN's decision-making avoids what is clearly a conflict of interest and preserves the stability and security of the DNS.

These concerns, as well as our suggested next steps, are described below as part of our comments on the GAC Advice.

Security and Stability Risks with new gTLDs

Over the last several years, ICANN's SSAC has correctly identified several critical issues that demand attention, mitigation and/or resolution prior to delegating new gTLDs into the root. These issues have been formally and publicly recorded in SSAC reports to the ICANN Board (SAC045, SAC046 and SAC057) but they have not, unfortunately, received the necessary levels of prompt attention and focus from ICANN and the community. As highlighted in Verisign's March 28, 2013, Verisign Labs Technical Report, "New gTLD Security and Stability Considerations," many of those issues remain open and require immediate attention to ensure the timely and responsible introduction of new gTLDs. Further detailed elaboration can be found in blog posts written by Verisign's Chief Security Officer: "Introduction: New gTLD Security and Stability Considerations" and "Internet Infrastructure: Stability at the Core, Innovation at the Edge." These are known issues and they must be addressed to in order to preserve the stability, security and resiliency of the DNS. To ignore known issues for the sake of expediency would be irresponsible and inconsistent with ICANN's core mission. It is crucial that the entire community, including governments and the GAC, ensure that the ICANN Board, ICANN staff and the SSAC remain focused on resolving these known issues.

The delegation of new strings in the root at this stage of the Internet's maturity may present substantial security risks because many existing applications and deployments have ossified the higher levels (e.g., root and TLDs) of the global DNS namespace. This is evident by the fact that these applications or deployments loosely tether themselves to the namespace by rigidly codifying "snapshots" of higher layers of the dynamic DNS structure directly into their

applications (e.g., Mozilla's http://suffixlist.org for privacy and security related to browsing and cookies). The delegation of many of the new gTLD strings into the root will present naming collision problems because some enterprise administrators are already using the same strings in their internal or alternative networks.

These issues are not new. In fact, since the early "Scaling the Root" studies in 2009, there have been recommendations for an assessment of these problems, which has to this day yet to occur. We are now at a critical point where it is imperative that such an assessment occur in order to understand the risks of delegating each new string into the root and the impact of potential naming collisions.

For example, if .corp is delegated into the root zone as a new gTLD, many believe that thousands or tens of thousands of enterprises could potentially be impacted. The problem is not just with obvious strings like .corp, but strings that have even small query volumes at the root may be problematic, such as those discussed in SAC045. These "outlier" strings with very low query rates may actually pose the most risks because they could support critical devices including emergency communications systems or other such life-supporting networked devices. Any such negative impacts would have serious consequences for those who rely on the DNS. We believe the GAC, and its member governments, would undoubtedly share our fundamental concern. Without some explicit understanding of second or third order effects and layered naming systems impacts, potential risks cannot, and will not, be fully understood until a delegation is made.

Accordingly, we believe it is critical that the GAC understand that Verisign strongly recommends that the following needs to occur as a matter of urgency and the highest priority:

1. An in-depth study and analysis needs to occur that involves instrumentation across the entire root server system in order to understand the consumption of all applied-for strings across a reasonable timeline to account for caching and other DNS ecosystem effects, with a focus on accuracy of results and dealing with the entire set of queries associated with applied for strings, not simply the ones that see the largest query volumes.
2. An early warning system must be made operational before delegation. Such a system must enable detection of various stresses on the system and implement the instrumentation noted above in order to understand how the root query characteristics change over time.
3. A policy framework is needed in order to codify a method for braking or throttling new delegations (if and when these issues occur) either in the DNS or in dependent systems that provides some consideration as to when removing an impacting string from the root will occur.

4. Before any new gTLD is delegated, each new string needs to undergo an appropriate assessment and study so that first-order risks are understood and determined to be acceptable before moving forward.
5. We submit that initially an ephemeral root delegation should occur for each new string with short but increasing lifetimes. Lower TTL values for DNS resource records associated with new strings will permit problematic high-impact delegations to be removed from the root as quickly as possible and the impact to be assessed before the delegation persists in the zone, as impacted parties will need time to adjust their infrastructure and systems in order to remediate problems that arise.
6. These steps should be in conjunction with the deployment of a well-publicized hotline and electronic communications medium staffed by well-trained experts to accept and assess newly identified risks as delegations proceed. This will enable the most prudent introduction of new gTLDs into the DNS and broader Internet ecosystem.

These issues are critically important to the stability of the Internet and must be addressed prior to delegation. We would welcome the opportunity to provide the GAC and/or GAC members with more information from our perspective regarding the ongoing security and stability risks associated with the New gTLD Program.

Safeguards Applicable to all New gTLDs

1. WHOIS verification and checks. The GAC recommends that registry operators conduct statistically significant checks to identify registrations with deliberately false, inaccurate or incomplete Whois data twice per year. As the GAC is no doubt aware, Section 3.7.8 of the 2013 Registrar Accreditation Agreement (RAA) requires registrars to conduct new, stringent initial and periodic Whois verification checks. Section 3.7.8 also imposes a new duty upon registrars to investigate and correct inaccurate Whois information. Thus, the GAC Advice is an additional check of Whois data, conducted by new gTLD applicants as registry operators and not registrars. It can be debated whether the GAC's advice is best implemented by amending the RAA to require registrars to conduct the new Whois checks, but if the GAC believes that registry operators should conduct these checks, we believe that the Registry Agreement (RA) could be amended to address this new registry operator duty. We also believe that new registries, together with ICANN, must convene a working group to specifically identify consistent criteria for conducting these checks. To this point, we have identified below some of the criteria that the working group should consider:

- Define the samples for domain names based on a definition of weighted statistical significance. There are many tools and algorithms available for registry operators to determine the required samples for twice yearly checks.
- Define the appropriate level of verification and check for Whois data. These levels may include increasing complexity and sophistication as outlined in the table below:

Level of Verification and Checks	Description	Examples
Basic Syntax	Check that the value of an entry complies with technical specifications	• Not blank entries for required fields such as postal address, email address, phone number • Consistent format of the entry with the intent of a specific field, such as a numeric zip code field that should only contain numbers
Semantic Validation	May include increasing level of validation from validation of individual data fields to consistency of multiple fields.	• Is the phone number listed (i.e., not 111-111-1111 or a U.S. phone number with a non-existing area code)? • Does the city exist? • Does the city exist within the state/country? • Does the street address exist within the city/state/country?
Individual/ Organizational Verification	Verify the names of individuals / organizations listed as the registrant / technical / administrative contacts and that these are associated with the additional contact information	• Investigation to verify accuracy of the contact names. This may be similar to identity verifications performed for Extended Evaluation Certificates • Verification that contacts are available at phone numbers and email addresses.

- As the level of verification and checks increases, this complexity will likely require registry operators to purchase and rely on third party services. While most

systems will support syntax validation, semantic validation requires access to authoritative data sources such as the U.S. Postal Service's Address Management System. Performing this type of validation would require a registry operator to incorporate these types of services for each country or jurisdiction applicable to their customer base.

- In order to manage a scalable, unbiased process to determine if data are deliberately inaccurate, the working group will need to define acceptable thresholds for data accuracy and consistency. These include criteria such as outdated data, typos, etc. For example, should the Whois record for a domain name be flagged as invalid if the registrant changed email providers even though the address and phone number are current?
- The costs incurred by the registry operator for Semantic Validation and Individual/Organizational Verification with global support will vary considerably. For example, many Certificate Authorities (CA) offer a range of SSL certificates from Standard to Extended Validation (EV) Certificates. A primary difference between these certificates is the level of identity verification. CAs charge hundreds of dollars per year more for EV Certs, which are issued according to a specific set of identity verification. Another verification benchmark for cost might be the validation level of effort and cost for the Trademark Clearinghouse. The Clearinghouse faces similar challenges in verifying data globally, although their process largely relies on publicly accessible records.
- The working group will need to develop a reporting and compliance mechanism to notify registrars of inaccurate or incomplete records.

It is important to note that while a gTLD registry could do these technical checks, any non-vertically integrated TLD can only validate that an address is formatted correctly and reachable/unreachable. A non-vertically integrated registry will never be able to authoritatively say that the registrant of that domain is accurately represented in the Whois data.

2. Mitigating Abuse Activity. The GAC recommends that registry operators ensure that the 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. Verisign believes that this advice could be implemented through the RA to require registry operators to pass through these terms to registrars and to registrants. Each of these prohibited activities should be defined in the RA with sufficient specificity to ensure consistent enforcement by registrars and registries for all new gTLDs.

3. Security Checks. The GAC recommends that registry operators conduct technical analyses to assess whether domains are being used to perpetrate security threats. The GAC further recommends that registry operators notify registrars of such activity and to suspend the domain name if the registrar does not take immediate action. We view this advice as imposing a new duty on registry operators that will require changes to the RA but only after careful study by a working group, and only in a manner consistent with the existing protections provided by legal precedent, including formalizing the definition of "security threats" and "cyber threats." We discuss briefly below two possible options for the community to consider. In either of the options discussed below, the registry operator will need to implement a system for registrar notification, technical support, and compliance. In cases that require suspension of a domain name, the Registry Registrar Agreement (RRA) must provide the appropriate terms and conditions for the registry operator to suspend the domain name while addressing concerns for privacy and confidentiality.

   Option 1. One option for conducting periodic technical analysis would be for the registry operator to contract with a security intelligence service or maintain a similar in-house capability. This service would monitor relevant vulnerabilities, malicious activity, global threats and cyber threat intelligence and provide actionable reports to the registry operator related to domain name use within their TLD.

   Option 2. An alternative would be for the registry operator to contract with an organization that has the ability to scan the domain names within the registry operator's TLD in order to identify security threats through detection of known malcode. In order for this to be effective, the registry would include terms in the RRA that would permit periodic scanning and prevent the registrar or third party hosting provider from blocking security scans by the registry operator.

   Because registries typically support registration of domain names at the second level, the security checks would logically be limited to security threats at this level. The registry should be cautioned about unexpected/undesirable consequences to dependent domain names and services when considering suspending second level domain names. Therefore, the registry operator will need to develop a system to identify dependencies, when possible. For example, if an email address at sample@gmail.com is being used to generate a phishing attack, suspending gmail.com may be the only action a registry could take but would have widespread impact and may not be the appropriate solution. Similarly, suspending second-level domain names used primarily as name servers by registrars and hosting companies could result in widespread unintended consequences. In most cases, the dependencies that are obvious with gmail, or domain names used

principally as name servers, are not discoverable by the registry. Therefore, cooperation with the relevant registrar is essential and should a registrar not take immediate action, the suspension may cause more harm than the known security threat.

4. Documentation. The GAC recommends that registry operators maintain statistical reports about the number of inaccurate Whois records and security threats and the action taken by the registry operator. The GAC further recommends that the reports be maintained for a defined contract period and to provide them to ICANN upon request. This new documentation and reporting obligation will require modifications to the Registry Agreement that detail the specific reportable items and the length of time to maintain such records and the conditions under which ICANN may request reports and the rights to use and protect the information in the report.

   Based on the intended use of these reports, the appropriate data may include a range of statistical metrics, from basic numbers of inaccurate Whois records or security threats over time, to more comprehensive information that would include statistics about types of inaccuracies or threats, actions taken by registrars and the registry operator.

   We believe that the working groups convened by ICANN to deliberate on the Whois and security checks should include this requirement as part of their charter.

5. Making and Handling Complaints. The GAC recommends that registry operators create a mechanism for making complaints to the registry operator that Whois information is inaccurate or that domain name registrations are being used to 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. This new mechanism would require modifications to the RA that detail the specific mechanism to be used by registry operators to implement this advice. One consideration for these modifications would be to segregate and define the appropriate processes for each type of complaint. For example:

   > Whois accuracy would most likely follow the system of verification and checks that the registry has implemented based on the requirements for Safeguard #1. Should the complaint arise for a Whois inaccuracy that is beyond the capabilities for the registry to manage, then the registry would need to provide guidance for the appropriate actions.
   >
   > The registry may define different processes for complaints regarding malware, botnets, and phishing, which may involve third parties such as the anti-phishing working group.

Complaints regarding activities that are subject to various legal jurisdictions pose a unique challenge for registry operators. Because registries do not have expertise in the laws of each jurisdiction from where a complaint may arise, a mechanism that registry operators may implement would be to provide guidelines to file the complaint in the appropriate jurisdiction.

6. Consequences. The GAC recommends that registry operators ensure there are real and immediate consequences for the demonstrated provision of false Whois information and for use of domain names in breach of applicable law including suspension of domain names. ICANN and registry operators must carefully consider the legal consequences of suspension and deletion of domain names. Verisign believes that ICANN should convene a working group that includes legal experts to study and make recommendation regarding any suspension and deletion policy. Such a policy must be appropriately tailored and must ensure that risks are appropriately allocated between ICANN, the registry operator, the registrar and registrants. Considerations for working group discussion may include, but are not limited to:

   Consideration of Whois information within the Registry operator verification capabilities, while verification of Whois accuracy that is beyond the scope of the Registry operator's capability may require referral to a third party, such as a registrar or independent identity verification organization.

   Consequences that are based on alleged claims related to a breach of applicable law may pose a significant risk to a registry operator, unless the action is directed by a court of competent jurisdiction. A registry operator would incur substantial risk by taking unilateral action against a domain name without appropriate indemnification. While registry operators should not be expected to interpret the applicable law by serving as judge and jury; the registry operator has the ability to implement court directed actions, such as putting a domain name on Hold (suspension of the domain name by removing it from the TLD zone file) or transferring the domain name between registrars.

   Registry operators may have similar policies and procedures in place today. These often require implementation of processes to receive orders, verify the domain names that are identified exist within the registry and the action directed is within the registry's capability. Registries may develop and maintain tools in order to effectively manage and implement the appropriate actions.

As with security and stability issues, implementing the GAC advice will require careful, bottom-up study to produce thoughtful recommendations. We acknowledge that some of the issues presented are complex. We strongly encourage ICANN to lead, and to organize community discussions, to consider and address both the security and stability risks and the GAC's important contribution to the new gTLD program.

Sincerely yours,

Patrick S. Kane
Senior Vice President
Naming and Directory Services
VeriSign, Inc.

Danny McPherson
Chief Security Officer
VeriSign, Inc.

APPENDIX

Safeguards for strings that are linked to regulated or professional sectors including the following 12 categories: Children, Environmental, Health & Fitness, Financial, Gambling, Charity, Education, Intellectual Property, Professional Services, Corporate Identifiers, Generic Geographic Terms, and Inherently Governmental Functions

#	Description	Recommended Implementation Action & Rationale
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.	ICANN should convene a working group to study how, if at all, registry, registrar and registration agreements should be amended to address this advice.
2	Registry operators will require registrars at the time of registration to notify registrants of this requirement.	See above.
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.	ICANN must identify with specificity what constitutes sensitive health and financial data and should provide guidance to registry operators to ensure this advice can be implemented. ICANN should ensure that any new security measures are implemented fairly and consistently through its agreements with registrars and registries.
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.	ICANN should ensure that registry operators are provided names of specific regulatory and industry self-regulatory bodies that apply to each category and should modify applicable registry agreements accordingly to account for this new requirement.

#	Description	Recommended Implementation Action & Rationale
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.	The RA and the RAA require abuse points of contact. We recommend that ICANN discuss this requirement with the GAC to ensure these existing obligations satisfy the GAC advice.
6*	At the time of registration, the registry operator must verify and validate the registrants' authorizations, charters, licenses and/or other related credentials for participation in that sector.	We recommend that these safeguards be implemented on a case by case basis as applicable via added registry agreement specifications. It seems likely that applicants of such gTLDs have already included such requirements in their registration procedures as described in their applications. There is precedent for implementing these kinds of requirements at the registry level in existing gTLDs (e.g., .jobs, .pro, etc.).
7*	Operators should consult with relevant national supervisory authorities, or their equivalents.	Similar to 6 above
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.	Same as 6 above

* Note that these safeguards only apply to a subset of the Category 1 strings, i.e., those that the GAC believes 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.

Safeguards for Specific Strings: .fail, .gripe, .sucks, .wtf

Description	Recommended Implementation Action
Develop clear policies and processes to minimize the risk of cyber bullying/harassment	We recommend that these safeguards be implemented on a case by case basis as applicable via added registry agreement specifications.

Category 2

Restricted Registration Policies

#	Description	Recommended Implementation Action
1	Registration restrictions for restricted access strings under Category 1 should be appropriate for the types of risks associated with the TLD. 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.	Transparency and equivalent access requirements are common to the domain registration industry so we suggest that such requirements be added to Registry Agreements on a case by case basis. For other parts of this safeguard we recommend that a joint GAC/GNSO group be formed to try to identify risks associated with specific strings and what types of restrictions might cause undue advantage, while taking into consideration business models that offer options like premium names or auctions..
2	For strings representing generic terms, exclusive registry access should serve a public interest goal.	ICANN should discuss this advice with the GAC to ensure that the "public interest" standard is defined and consistently applied.