



The Internet Corporation for Assigned Names and Numbers

January 25, 2012

The Honorable Barbara Boxer
United States Senate
112 Hart Senate Office Building
Washington, D.C. 20510

The Honorable Olympia Snowe
United States Senate
154 Russell Senate Office Building
Washington, D.C. 20510-1903

The Honorable Maria Cantwell
United States Senate
311 Hart Senate Office Building
Washington, DC 20510

The Honorable Mark Warner
United States Senate
475 Russell Senate Office Building
Washington, DC 20510

The Honorable Claire McCaskill
United States Senate
Hart Senate Office Building, Ste. 506
Washington, D.C. 20510

Dear Senators Boxer, Cantwell, McCaskill, Snowe and Warner:

Thank you for your consideration of ICANN's New gTLD Program and for allowing ICANN to expand on our testimony provided before the Senate Commerce, Science, and Transportation's hearing on December 8, 2011. Attached please find ICANN's responses to the written questions for the record.

Sincerely,

Kurt J. Pritz
Senior Vice President, Stakeholder Relations

Marina del Rey
Brussels
Sydney
Washington, DC

4676 Admiralty Way, Suite 330
6 Rond Point Schuman, Bt. 5
Level 2, 48 Hunter Street
1875 I Street, NW, 5th Floor

Marina del Rey, CA 90292
B-1040 Brussels
Sydney NSW 2000
Washington, DC 20006

USA
BELGIUM
AUSTRALIA
USA

T +1 310 823 9358
T +32 2 234 7870
T +61 2 8236 7900
T +1 202 429 2704

F +1 310 823 8649
F +32 2 234 7848
F +61 2 8236 7913
F +1 202 429 2714

**Senator Barbara Boxer
Commerce, Science, and Transportation Committee
Questions for the Record
“ICANN’s Expansion of Top Level Domain Names”
December 8, 2011**

To Mr. Kurt Pritz, Senior Vice-President, ICANN

Question 1

Intellectual property rights holders have expressed some concerns about the possibility of ICANN granting generic top-level domain names (gTLDs) that could lead to consumer confusion, or violations of trademark or other intellectual property rights. Could you describe, in detail, the pre-grant procedures by which ICANN will act to prevent gTLDs that could cause consumer confusion and/or violation of intellectual property rights?

Answer to Question 1

The New gTLD Program contains a suite of new, mandatory intellectual property rights protection mechanisms, both at the first level (for the top-level domains, or names to the right of the dot such as .org) and at the second level (second-level domains, like icann.org). The first level protections mitigate against applications for and the approval of new TLDs that may infringe on the legal rights of others or cause consumer confusion.

First, there is a high bar to participation in the Program. The \$185,000 evaluation fee itself is a bar to potential wrongdoing at the top-level.¹ In today’s environment, second-level domain names are available for \$10. Wrongdoers easily leave them behind when the site is exposed. The higher evaluation fee for top-level names in itself will discourage abuse.

Second, the stringent reviews include measures specifically targeted to identify – and reject – applicants that are bad actors or have already demonstrated a history of cybersquatting. ICANN requires background reviews of TLD applicants, including reviews for criminal history (including the use of telecommunications or the Internet to facilitate crimes, illegal sale of drugs, and others). In addition, ICANN will reject applications where the applicant has a pattern of adverse decisions under the UDRP (Uniform Domain Name Dispute Resolution Policy), or has been found to act in bad faith or with reckless disregard to their obligations under cybersquatting legislation.

Third, the Program offers public review of the applied-for strings and the opportunity to state an objection to any string. After the April 12, 2012 close of the application window, ICANN will publish a list of all applied-for gTLDs. (That publication will occur around May 1, 2012.) At that time, entities, individuals and governments can review the list of strings and consider if they wish to object to any individual application. In addition, the New gTLD Program allows ICANN’s Governmental Advisory Committee, comprised of representatives of over 120 governments, to inform ICANN that there are concerns with an application – concerns that may include issues of consumer confusion or harm. If the Governmental

¹ The fee was calculated based on a cost recovery model but the amount has the side benefit of deterring frivolous or malicious applications.

Advisory Committee provides consensus advice to the Board not to approve and application, that advice creates a presumption in favor of denying the application.

There are four formal objection processes that can be initiated by the public, each administered by a well-known international dispute resolution service provider. Types of objections that can be lodged are:

- String Confusion Objection – The applied-for gTLD string is confusingly similar to an existing TLD or to another applied for gTLD string in the same round of applications.
- Legal Rights Objection – The applied-for gTLD string infringes the existing legal rights of the objector.
- Limited Public Interest Objection – The applied-for gTLD string is contrary to generally accepted legal norms of morality and public order that are recognized under principles of international law.
- Community Objection – There is substantial opposition to the gTLD application from a significant portion of the community to which the gTLD string may be explicitly or implicitly targeted.

To avoid frivolous objections, parties must have standing to object. For example, legal rights objectors must be the right holder or intergovernmental organization whose rights are being infringed.

Objections lead to independent dispute resolution proceedings. Parties are the objector and the gTLD applicant.

- The International Centre for Dispute Resolution has agreed to administer disputes brought pursuant to string confusion objections.
- The Arbitration and Mediation Center of the World Intellectual Property Organization has agreed to administer disputes brought pursuant to legal rights objections.
- The International Center of Expertise of the International Chamber of Commerce has agreed to administer disputes brought pursuant to Limited Public Interest and Community Objections.

Standards of review for each of the objections have been carefully crafted through reviews by intellectual property holders and the Internet community. For example, in the case of rights infringement objections, “Strings” must not infringe the existing legal rights of others that are recognized or enforceable under generally accepted and internationally recognized principles of law. A Dispute Resolution Service Provider panel of experts presiding over a legal rights objection will determine whether the potential use of the applied-for gTLD by the applicant takes unfair advantage of the distinctive character or the reputation of the objector’s registered or unregistered trademark or service mark (“mark”) or IGO name or acronym (as identified in the treaty establishing the organization), or unjustifiably impairs the distinctive character or the reputation of the objector’s mark or IGO name or acronym,

or otherwise creates an impermissible likelihood of confusion between the applied-for gTLD and the objector's mark or IGO name or acronym.

In the case where the objection is based on trademark rights, the panel will consider the following non-exclusive factors:

1. Whether the applied-for gTLD is identical or similar, including in appearance, phonetic sound, or meaning, to the objector's existing mark.
2. Whether the objector's acquisition and use of rights in the mark has been bona fide.
3. Whether and to what extent there is recognition in the relevant sector of the public of the sign corresponding to the gTLD, as the mark of the objector, of the applicant or of a third party.
4. Applicant's intent in applying for the gTLD, including whether the applicant, at the time of application for the gTLD, had knowledge of the objector's mark, or could not have reasonably been unaware of that mark, and including whether the applicant has engaged in a pattern of conduct whereby it applied for or operates TLDs or registrations in TLDs which are identical or confusingly similar to the marks of others.
5. Whether and to what extent the applicant has used, or has made demonstrable preparations to use, the sign corresponding to the gTLD in connection with a bona fide offering of goods or services or a bona fide provision of information in a way that does not interfere with the legitimate exercise by the objector of its mark rights.
6. Whether the applicant has marks or other intellectual property rights in the sign corresponding to the gTLD, and, if so, whether any acquisition of such a right in the sign, and use of the sign, has been bona fide, and whether the purported or likely use of the gTLD by the applicant is consistent with such acquisition or use.
7. Whether and to what extent the applicant has been commonly known by the sign corresponding to the gTLD, and if so, whether any purported or likely use of the gTLD by the applicant is consistent therewith and bona fide.
8. Whether the applicant's intended use of the gTLD would create a likelihood of confusion with the objector's mark as to the source, sponsorship, affiliation, or endorsement of the gTLD.

For a complete description of the standards and rules for the objection and dispute resolution processes, see Module 3 of the Applicant Guidebook, <http://newgtlds.icann.org/en/applicants/agb/objection-procedures-11jan12-en.pdf>.

In addition, there will be a specialized function, an "Independent Objector" that will act solely in the best interest of the public, and may file an objection to an application that may give rise to the concerns raised above.

As noted at the Subcommittee hearing, some trademark holders continue to voice concern that the New gTLD Program does not offer sufficient protections to reduce the need to

submit defensive applications for top-level domains. Detailed discussions with intellectual property experts that participate actively in ICANN policy development indicate that those experts who are knowledgeable of the TLD marketplace are most comfortable with protections for top-level names. In regards to the perceived need for defensive registrations at the top-level by trademark holders, ICANN has already committed to solicit information as expeditiously as possible from the intellectual property community. This commitment, set out in a January 11, 2012 letter to Assistant Secretary for Communications and Information, Lawrence Strickling, also committed ICANN to submit any new proposals or recommendations arising out of that work for evaluation and comment from the ICANN stakeholder community.

Question 2

It is my understanding that in previous expansions of domain names, ICANN has allowed a “sunrise” period, prior to considering applications, in order to allow rights holders to submit information regarding their protected names and uses. The “sunrise” submissions by rights holders could act as a resource for ICANN to help prevent consumer confusion and/or intellectual property rights violations. Does ICANN plan to allow “sunrise” submissions by rights holders, and if not, why?

Answer to Question 2

Yes, a “sunrise” period is mandated for each new TLD approved under the New gTLD Program.

ICANN is in the process of selecting providers for a Trademark Clearinghouse, a central repository for information to be authenticated, stored, and disseminated pertaining to the rights of trademark holders. Trademark holders will have the opportunity to record (i) Nationally or multi-nationally registered word marks from all jurisdictions; (ii) Any word mark that has been validated through a court of law or other judicial proceeding; (iii) Any word mark protected by a statute or treaty in effect at the time the mark is submitted to the Clearinghouse for inclusion; and (iv) other marks that constitute intellectual property, all subject to the specific criteria of the Clearinghouse.

The authenticated rights data in the Trademark Clearinghouse will be used to support pre-launch Sunrise and Trademark Claims services. All new gTLD registries will be required to use the Trademark Clearinghouse to support the required pre-launch and initial launch period rights protection mechanisms that must include, at minimum, a Trademark Claims service and a Sunrise process.

The Trademark Clearinghouse is expected to create efficiencies and for trademark holders. Instead of requiring trademark holders to authenticate mark information for each separate new registry, the authentication and validation processes can be completed once through submission to the Trademark Clearinghouse.

Through the Sunrise process, trademark holders will have the opportunity to register desired second-level domain names before a new gTLD opens for general registration. Rights holders who have recorded their data in the Trademark Clearinghouse will receive notice if a third party registers a domain name matching the Clearinghouse record during the sunrise period.

After the gTLD is accepting general registrations, ICANN requires that each new TLD offer a Trademark Claims service to provide real-time notices to prospective registrants where a domain name matches a Clearinghouse record, and provide notice to trademark holders in cases where domain names matching a Clearinghouse record are registered. Information on the additional intellectual property protections required under the New gTLD Program is detailed in my written testimony.²

² A summary of the trademark protections is available at <http://www.icann.org/en/topics/new-gtlds/rights-holders-with-insert-02sep11-en.pdf> and <http://www.icann.org/en/topics/new-gtlds/trademark-factsheet-insert-02sep11-en.pdf>.

**Senator Maria Cantwell
Commerce, Science, and Transportation Committee
Questions for the Record
“ICANN’s Expansion of Top Level Domain Names”
December 8, 2011**

Questions for Mr. Pritz

Question #1 – DNS Security

Mr. Pritz, my understanding is that all of the new domains that will be selected by ICANN must agree to use the Domain Name System Security Extensions, known as DNS SEC. DNS SEC uses public key cryptographic digital signatures to authenticate the origin of the DNS data and assure the integrity of the DNS data.

- Currently, are DNS servers and DNS server software targeted for attack by hackers?
- Why is DNS SEC important to any broader global cyber-security effort?
- Does DNS SEC allow for any re-direction in its current implementation? Could it be made to? What would be some of the potential security vulnerabilities if DNS SEC were to allow any redirection?
- What is the status of DNS SEC implementation with respect to existing domains? Is it realistic to expect that the new domains will be compliant right from the start?

Answer to Question 1

Today, DNS servers and server software are targeted for attack by hackers. There are recent examples of incidents in which hackers were able to impersonate DNS server responses, or feed false data to the servers, ultimately redirecting end users to rogue sites to install malware. For example, the “DNS Charger” case – recently the subject of an indictment in the Southern District of New York, infected over 4 million computers worldwide through this type of attack.

Coordinated deployment of DNSSEC is important in many respects. First, it will protect against attacks on DNS servers and software. Possibly even more important, however, the borderless nature of DNSSEC deployment has – for the first time – created a global, cross-organizational, trans-national platform for authentication, cyber security innovation and international cooperation. This will make DNSSEC a critical tool in combating the global nature of cyber crime.

DNSSEC does not allow for re-direction in its current implementation. Re-direction requires a change to the original record by a third party. With DNSSEC, any changes to the original record from the domain name owner’s servers will be detected and flagged as an

error or dropped. The validation occurs on the end user's machine to provide true end-to-end security.

Any change to DNSSEC to allow for re-direction would defeat its purpose. The purpose of DNSSEC is to use digital signatures to ensure records do not get changed "in flight." An alternative could be to put full trust in your Internet service provider (ISP) to perform the validation and enter manual re-direction entries, however this appears to be an inadequate level of security. For example, in late 2011, an attack on servers at multiple Brazilian ISPs caused redirection to malware-infected sites before connecting the ISP's customers to popular Internet sites.³ This affected millions of users, and demonstrates that leaving validation to the ISP level is insufficient to protect against attacks.

If DNSSEC were to allow re-direction or filtering, that would make the system again vulnerable to insider attacks. In addition, re-direction could lead to poor performance due to the processing of large re-direction lookup tables for the billions of DNS queries that happen each day, as well as undesired responses. Re-direction could result – with one click – permanently leading the end user to use alternate, unfiltered and insecure non-DNSSEC validating servers.

DNSSEC adoption is growing. Today, 82 top-level domain name registries (covering 82% of existing domain names), including .COM and .ORG, have DNSSEC deployed. The new gTLD Program requires that all new registries deploy DNSSEC. In the United States, Comcast has begun rolling out DNSSEC to all 17.8 million of its Internet customers⁴, and internationally, we've seen adoption by network carriers such as Vodafone and Telefonica. It is realistic that new TLDs will be compliant from their introduction, as required in the Program. It is not a difficult requirement to meet, and current products, including hardware have DNSSEC support built in. ICANN and other organizations are regularly running training and awareness sessions to increase DNSSEC adoption.

Question #2 – Cracking down on rogue websites

Mr. Pritz, do you believe that the increase in top level domains combined with all the requirements ICANN is putting in place will make it easier, more difficult, or not change the ability of U.S authorities to crack down on Internet sites -- to use the phrase – that are dedicated to infringing activity?

Answer to Question #2

The New gTLD Program includes protections (not required in today's TLD), designed to prevent malfeasance and to make it easier to crack down on malicious conduct where it

³ See e.g., "Hackers poison Brazilian ISP DNS to infect users with banking Trojan," TECHWORLD, Nov. 9, 2011 at <http://news.techworld.com/security/3317148/hackers-poison-brazilian-isp-dns-to-infect-users-with-banking-trojan/>.

⁴ See, "Comcast Completes DNSSEC Deployment," by Jason Livingood, Vice President, Internet Systems, January 10, 2012 at <http://blog.comcast.com/2012/01/comcast-completes-dnssec-deployment.html>.

occurs. Some of the tools directly relating to increased law enforcement access to information and ability to combat malicious conduct in new TLDs include:

- A requirement to maintain enhanced, or “thick”, WHOIS records at the registry level to allow more rapid search capabilities, facilitating efficient resolution of malicious conduct activities;
- A centralized zone file access system to allow for more accurate and rapid identification of key points of contact within each gTLD. This reduces the time necessary to take corrective action within TLDs experiencing malicious activity; and
- A requirement to establish a single point of contact responsible for the handling of abuse complaints (as requested by law enforcement authorities).
- Background reviews of TLD applicants, including reviews for criminal history (including the use of telecommunications or the Internet to facilitate crimes, illegal sale of drugs, and others);
- Rejection of applications where the applicant has a pattern of adverse decisions under the UDRP (Uniform Domain Name Dispute Resolution Policy), or has been found to act in bad faith or with reckless disregard to their obligations under cybersquatting legislation;
- The requirement to have a plan to implement domain name system security extensions (DNSSEC), reducing the risk of “man-in-the-middle” attacks and spoofed DNS records; and
- Requirements that New gTLD Registry Operators must:
 - Maintain a Continued Operations Instrument sufficient to fund basic registry operations for a period of three years in case of business failure, to protect consumers and registrants within that gTLD in the event of registry failure.
 - Maintain continuity and transition plans, including regular failover testing.
 - Cooperate with ICANN In the event transition to a new registry operator is necessary. ICANN will identify an Emergency Back-End Registry Operator to assist in the registry transition process and provide emergency registry services as needed.

In addition, ICANN is actively working to address 12 recommendations made by law enforcement regarding strengthening ICANN’s contracts with its accredited registrars. Specifically, as directed by the Board, ICANN is currently in negotiations with its accredited registrars to amend the Registrar Accreditation Agreement (RAA) to meet the

recommendations raised by law enforcement authorities. Amendments are expected to be in force prior to the entry of the first new gTLD in 2013.

These negotiations include face-to-face meetings with law enforcement agencies to ensure understanding of law enforcement requirements. The negotiation anticipates substantial and unprecedented steps to improve the accuracy of Whois data. ICANN is taking a strong stand in regard to issues relating to the verification of Whois data and expects the accredited registrars to take action to address the demands of governments and law enforcement worldwide. Updates on the negotiations are available at <https://community.icann.org/display/RAA/Negotiations+Between+ICANN+and+Registrar+s+to+Amend+the+Registrar+Accreditation+Agreement>.

Question #3 -

- Mr. Pritz, how many new gTLD and other domains does ICANN estimate will be created?
- What is the process by which ICANN will award the new gTLD and other domains? Will it be just a matter of who can bid the most?
- How much money is expected to be raised from the new gTLDs and other domains?
- What does ICANN intend to do with the funds? What are the mechanisms in place to assure accountability?

Answer to Question 3

The number of new gTLDs that will be created through this first application round is still a matter of speculation. Early estimates coming from the community postulated that there would be 500 or more applications. Recently, some have estimated that 1000 or more applications will be made in the current round, opened on January 12, 2012. Once the application window closes on April 12, 2012, the speculation will come to an end and the full number of applications will be known. Not surprisingly, many companies are remaining quiet about their business strategies regarding plans to establish new gTLDs, making true estimates difficult.

If significantly more than 500 applications are received, the applications will be processed in batches of 500. In addition, on the advice of root server stability experts, ICANN has committed to limit the number of new TLD entered into the root in any one year to 1,000.

The extensive application and evaluation process is set out in the *Applicant Guidebook*, with over 300 pages of detail. Applicants must meet all of the application criteria, pass the rigorous evaluations, as well as pass through any of the four objection processes that may be used against the application. The key to the application process, however, is that it does not create a beauty contest among applicants or impose arbitrary limitations such as type

of application that existed in two prior pilot rounds on new gTLDs. These pilot rounds are described in detail in response to Senator McCaskill's question 2.

All applicants are expected to pay the \$185,000 evaluation fee to ICANN, unless the applicants qualify for financial support. If an applicant qualifies for the available financial support, it will only pay \$47,000 towards the application fee. The \$185,000 application fee is calculated on a cost-recovery model, and was determined through a comprehensive and complex process that included identifying over 100 separate tasks required for the evaluation of a new gTLD application and seeking guidance from experts. The fee includes development costs (\$26,950 per application); application processing and evaluation costs (\$97,800 per application); and costs for risk mitigation steps, including allowance for unanticipated costs and variations between estimates and actual costs incurred (\$60,000 per application). A 14-page document setting out the methodology and further breakdown of the fee component is available at <http://www.icann.org/en/topics/new-gtlds/cost-considerations-04oct09-en.pdf>. This document is an update to the earlier "Cost Considerations of the New gTLD Program", published in October 2008, available at <http://www.icann.org/en/topics/new-gtlds/cost-considerations-23oct08-en.pdf>.

While there is a possibility that multiple applicants for the same TLD could proceed to an auction to operate the TLD, ICANN intends the auction process as a last-resort method. ICANN encourages applicants to work together to arrive at a mutually-agreeable solution instead of allowing the competing applications to proceed to an auction. To the extent that a TLD proceeds to auction and generates additional funds, I discuss below ICANN's commitments to using these funds towards its not-for-profit mission.

As a Not-for-Profit Public Benefit Corporation, ICANN is committed to its not-for-profit mission. For ICANN, that commitment requires us to assure that excess funds generated through the New gTLD Program (i.e., those that exceed the costs incurred for the processing, evaluation and other components of the New gTLD Program) are used in furtherance of ICANN's mission. The evaluation fee has been calculated to recover costs and not exceed those costs. If evaluation fees exceed actual costs, future evaluation fees will be reduced. If costs exceed fees, then ICANN will absorb that and future fees will be increased to meet the actual costs. For additional funds accruing to ICANN other than evaluation fees, such as the auction proceeds mentioned, the *Applicant Guidebook* addresses the issue in this way:⁵

It is planned that costs of the new gTLD program will offset by fees, so any funds coming from a last resort contention resolution mechanism such as auctions would result (after paying for the auction process) in additional funding. Any proceeds from auctions will be reserved and earmarked until the uses of funds are determined. Funds must be used in a manner that supports directly ICANN's Mission and Core Values and also allows ICANN to maintain its not for profit status.

⁵ See Module 4, Page 19 of the *Applicant Guidebook*, version 2010-01-11.

Possible uses of auction funds include formation of a foundation with a clear mission and a transparent way to allocate funds to projects that are of interest to the greater Internet community, such as grants to support new gTLD applications or registry operators from communities in subsequent gTLD rounds, the creation of an ICANN-administered/community-based fund for specific projects for the benefit of the Internet community, the creation of a registry continuity fund for the protection of registrants (ensuring that funds would be in place to support the operation of a gTLD registry until a successor could be found), or establishment of a security fund to expand use of secure protocols, conduct research, and support standards development organizations in accordance with ICANN's security and stability mission.

ICANN handles its budgeting processes in an open and transparent manner. Not only will the community discussion regarding the use of excess funds be the subject of community consultation, but the funds will also be tracked and accounted for within ICANN's publicly-posted financial documents.

Senator Claire McCaskill
Commerce, Science, and Transportation Committee
Questions for the Record
“ICANN’s Expansion of Top Level Domain Names”
December 8, 2011

1. To Kurt Pritz and Dan Jaffe:

I recognize that ICANN has put a tremendous amount of work and study into the planned expansion of top-level domain names. There have been a number of economic studies, dozens of comment periods and seven versions of the Applicant Guidebook before the final one was issued. ICANN clearly views the expansion of gTLDs as vital to the growth and viability of the Internet.

Given how much time, effort and study has been put into this decision, I find it disturbing that there is still so much dispute about expansion. There is clearly a lack of consensus about these changes in the business and non-profit industries as well as concerns from law enforcement. This is not a decision to be taken lightly and I believe there needs to be better agreement on the outstanding issues from all interested parties.

Both of you have very differing opinions about the implications of the gTLD expansion. Why has it taken this long to get this out in the open?

Mr. Jaffe, there was an extensive comment period before the guidelines were issued, which I’m sure you were aware of—did you and other industries fully participate in the process? Do you disagree with the economic studies that ICANN has cited saying this would increase competition and innovation? If so, why?

Mr. Pritz, how much weight was given to the concerns raised by Mr. Jaffe and others with his viewpoints? The danger of increased copyright infringement appears to be a legitimate issue—do you agree?

Answer to Question 1

Formation of rights protection mechanisms for the new gTLDs has been an important, legitimate concern throughout the development of the New gTLD Program.

The years of policy and implementation design work that have gone into the New gTLD Program have formed a program that will result in TLDs that are required to offer more protections than TLDs that have already been introduced into the Domain Name System. The program was designed over more than six years, with input from no less than ten independent expert and community working groups addressing the issues that ANA continues to raise outside of the multi-stakeholder process. There are significant trademark protections designed by intellectual property experts. There are substantial protections against registry failure, including requirements for registry transition planning

and designation of emergency registry operators, so that even in the event of registry failure, consumers will have a period of three to five years until basic registry operations are concluded.

One of the hallmarks of ICANN is its ability to call together world-class experts to consider issues facing the ongoing stability and security of the Internet. For the new gTLD program, ICANN formed teams of: intellectual property experts to develop trademark protection mechanisms; Internet security experts to develop consumer protections; registry operators to create mechanisms to access registry data; financial services providers to develop thresholds for “secure” TLDs; and linguists to avoid user confusion.

In addition to those ten independent expert working groups formed, ICANN published, 59 explanatory memoranda and independent reports, thousands of comments in no fewer than 47 extended public comment periods, and 1400 pages of comment summary and analysis as part of the community formation of the New gTLD Program. All comments were listened to and taken into account across the eight versions of the *Applicant Guidebook*. All of the rights protection mechanisms were borne of these community consultations.

The Association of National Advertisers is just one of the hundreds of voices that participated in the formation of the New gTLD Program. The ANA provided feedback using ICANN’s public comment process, and its suggestions have been carefully considered as described below. Referring to the comment submitted by the ANA on 15 December 2008, that letter stated:

“Although ANA would have preferred ICANN to have decided against introducing the gTLD proposal, we urge, at a minimum, that ICANN move cautiously and consider points carefully before embarking on this potentially seismic shift in domain availability.”

The letter suggested five specific proposals that ICANN should, at a minimum, consider:

1. Protections for Trademarks. ICANN should explore additional application restrictions, processes and technologies to insulate brand owners from the costs and burdens of chasing and prosecuting squatters and others for violation of their trademark rights.

In response to this and similar comments, ICANN convened the Implementation Response Team (comprised of 18 intellectual property experts) to recommend additional trademark protections, as discussed within my testimony. The majority of those recommendations have been incorporated, many in a stronger form than was originally proposed by the IRT.

2. Transparency of Applications and Registration Information. Some comments suggest transparency in the application process (e.g., elimination of proxy registrations, heightened emphasis on the provision of complete “whois” information, and posting all gTLD applications) will lead to less abuse. ICANN should examine these proposals as well.

In response to this and other comments: (1) more application information will be made public in the process of publishing information about the applied-for strings (personally

identifiable information and sensitive security or proprietary information are not published), (2) background checks on applicants have been deepened, and (3) all new gTLD registries are required to maintain a “complete” or “thick” Whois model. As discussed in response to Senator Cantwell’s Question 1, work to require verification of Whois information is underway through ICANN’s negotiations with its registrars on the Registrar Accreditation Agreement. Those verification requirements are expected to be in place prior to the entry of the first new gTLD.

3. Fees. ICANN should study the various issues raised concerning fees, including those questions relating to how the new proposed fee structure might impact fee structures with existing gTLDs.

In response to this and other comments, fee structures have been extensively studied. The process used for estimating fees has been available since October 2008 and was iterated in response to public comment, and an economic study was undertaken on registry competition and price caps, which supported that price caps should not be introduced within new TLDs absence a showing of market power. A detailed discussion regarding the fee structure is provided in response to Senator Cantwell’s Question 2.

4. General Process Issues. ANA notes several application and adjudication process issues that should be analyzed, including ICANN’s right to “overrule” the determination of a Dispute Resolution Provider, the apparent absence of judicial remedy and how allowing public comments on the application process impacts it as a whole and, particularly, the objection process.

In response to this and other comments, elaborations were made to the objection processes, and the roles of the Board, governments, and public comment have been clarified. As discussed in my response to Senator Boxer’s Question 1, the objection processes are robust and well-defined.

5. “Generic” gTLDs (e.g., .bank, .insurance, .securities, .medicine, etc.) have a unique social and commercial value as they are broadly descriptive of industries and other unifying activities. Under the terms of the Draft RFP, anyone can apply for these “generic” gTLDs, including a single member of the applicable industry. ANA suggests that ICANN thoroughly review the uses and standing requirements for these gTLDs.

In response to this and other comments, and in particular working with BITS (the policy division of The Financial Services Roundtable) and the financial services industry, a requirement was added that security capabilities should be commensurate with the nature of the string, i.e., applications for strings with unique trust implications are expected to provide a commensurate level of security. Applicants are also given incentive to incorporate security levels that exceed the baseline requirements. The gTLD criteria also references work independently published by the American Bankers Association and The Financial Services Roundtable as an illustrative example of how the criteria for a high-security TLD could be satisfied. In the event that a string is applied for and does not include appropriate security measures, that could serve as the basis for objection or an issuance of a GAC Early Warning regarding the string (a process where governments,

through the Governmental Advisory Committee, provides notice regarding potential sensitivities with an application).

As seen from ICANN's responses, all of the ANA's comments were considered, responded to, and, as is clear from the above, largely accepted. This is indicative of the process that was followed with all stakeholder comment on the New gTLD Program to arrive at a balanced outcome.

The broad consensus work that went into the development of this program does not mean that everyone is satisfied with the result. There are some who wish for more restrictions; some for less. Lawrence Strickling, Assistant Secretary of Commerce for Communications and Information of the National Telecommunications and Information Agency, U.S. Department of Commerce, recently described the process of building consensus in ICANN's multistakeholder model, as well as the importance of respecting the outcomes reached, noted that while the multistakeholder process does not guarantee that everyone will be satisfied with the outcome, it is critical to respect the process and accept the outcome reached.⁶

ICANN's opening of the application window for new TLDs is in fulfillment of ICANN's role of accountability to the outcomes of the multistakeholder model. ICANN remains accountable to evaluation of the expansion and implementing refinements to the New gTLD Program that may arise through the multistakeholder model.

With the opening of the application window, ICANN's work continues. ICANN has already committed to solicit information as expeditiously as possible from the intellectual property community. This commitment, set out in a January 11, 2012 letter to Assistant Secretary for Communications and Information, Lawrence Strickling, also committed ICANN to submit any new proposals or recommendations arising out of that work for evaluation and comment from the ICANN stakeholder community.

ICANN has already committed to review the impacts of the rollout of the New gTLD Program, including a post-launch study on the effectiveness of the new trademark protections and any effects on root zone operations, and a post-delegation economic study on the results of the first set of new gTLDs. ICANN has also committed to undertake reviews in accordance with the Affirmation of Commitments between the United States Department of Commerce and ICANN, including a review "that will examine the extent to which the introduction or expansion of gTLDs has promoted competition, consumer trust and consumer choice, as well as effectiveness of (a) the application and evaluation process, and (b) safeguards put in place to mitigate issues involved in the introduction or expansion." There will be opportunities for public input regarding all of this post-launch work.

⁶ Remarks of Assistant Secretary Strickling at the Practising Law Institute's 29th Annual Telecommunications Policy & Regulation Conference, December 8, 2011, available at <http://www.ntia.doc.gov/speechtestimony/2011/remarks-assistant-secretary-strickling-practising-law-institutes-29th-annual-te>.

ICANN looks forward to ICANN and Internet community members continuing their involvement within the multi-stakeholder model and bringing their proposals for discussion among all of the Internet's stakeholders.

2. To Kurt Pritz:

I know that ICANN is resistant to limiting the number of new gTLDs because it does want to pick winners and losers about which gTLDs should be added. But prior expansions have been limited. What are the concerns now of trying a pilot or more limited expansion to examine problems that may occur in the process?

Answer to Question 2

ICANN has operated three pilot programs on the introduction of new TLDs into the DNS. In 2000, ICANN launched a "Proof of Concept" round, through which seven new TLDs were selected out of 44 applicants who proposed over 200 different potential TLDs. In 2004, ICANN accepted applications for Sponsored Top-Level Domains (sTLDs), specialized TLDs that are tied to defined sponsor communities (such as .CAT for the Catalan-speaking community). Finally, ICANN launched the Internationalized Domain Name country code TLD (IDN ccTLD) Fast Track process in 2009 that, to date had resulted in the delegation of 30 IDN TLDs, enabling countries and territories that use languages based on scripts other than Latin to offer users domain names in non-Latin characters (e.g., Arabic, Chinese, Devanagari, Russian, Thai scripts).

Through these pilot rounds, important lessons were learned. First, new TLDs can safely be added to the DNS. Second, the imposition of artificial restrictions on the rounds, such as the numerical restriction imposed in 2000 and the type-restriction imposed in 2004 place ICANN in the position of picking winners and losers, as opposed to fulfilling its mission of facilitating competition in the DNS. Artificial restrictions also create incentives for applicants to work to fit their TLD ideas into categories that may not be a true fit. The outcomes of the pilot rounds also helped inform the heightened protections in place for the New gTLD Program. The pilot programs informed the creation of independent dispute resolution programs that anticipate points of contention and provide paths for addressing potential abuses, controversies and sensitivities. The Fast Track program (and the IDN test bed before that) demonstrates that IDNs can be safely delegated into the root zone. These lessons learned will enable the realization of anticipated benefit in a safer environment.

The New gTLD Program will be implemented in a measured and limited manner. Rather than limiting by number or type, the round is limited by a high bar of required competencies and protections, and a limited application period. There is a 90-day application window, followed by a stringent evaluation process through which ICANN's expert evaluation panels will evaluate registry abilities to meet the high technical and operational requirements. The rollout of new gTLDs will be distributed over time – no TLDs are expected to be operational prior to early 2013; delegations of additional TLDs will be distributed after that, as the applications pass through the evaluation and dispute resolution processes. The imposition of otherwise artificial limitations on today's New

gTLD Program would only create incentives for the bad-acting applicants to seek advantages in a subjective evaluation process. The Program in place today allows applicants to be evaluated against objective standards.

As part of the consensus-building process, ICANN has agreed with governments and trademark holders that the next round of new TLD applications should occur after studying the impact of this round 's delegations on root zone stability and conducting a study on whether new trademark protections should be adjusted. ICANN will undertake these studies as soon as is practicable, in consultation with stakeholders. ICANN will also provide public updates on the ongoing process to determine the timing of the next round.

ICANN is also mindful of its commitments set forth in the Affirmation of Commitments to, "organize a review that will examine the extent to which the introduction or expansion of gTLDs has promoted competition, consumer trust and consumer choice, as well as effectiveness of (a) the application and evaluation process, and (b) safeguards put in place to mitigate issues involved in the introduction or expansion."⁷

3. To Kurt Pritz:

I recognize that ICANN believes all of the issues have been fully vetted and that everyone has had ample time to state their views. But given the major disagreements that are still occurring, what is the harm in delaying implementation to further work through these issues in the hope of coming to a better consensus? In your view, what would happen if ICANN does not start the expansion process in January?

Answer to Question 3

On January 12, 2012, ICANN opened the first application window for new gTLDs. As discussed within my written testimony, the opening of the application window is only the first step to rolling out new gTLDs, with the first new gTLD expected to be operational until 2013.

ICANN's opening of the application window in accordance with the timeframe committed to in June 2011 was an important step in remaining accountable to the Internet community. As noted above, work is still ongoing – the Program will be subject to continued reviews and refinements. However, with the years' worth of work already completed, the ten independent expert working groups, 59 explanatory memoranda and independent reports, thousands of comments in no fewer than 47 extended public comment periods, and 1400 pages of comment summary and analysis, it was time for the Program to move into implementation so that the Internet community can start analyzing its effects using true data and experience.

⁷ See <http://www.icann.org/en/documents/affirmation-of-commitments-30sep09-en.htm>.

Delaying the process serves those seeking to upset the multi-stakeholder model, designed by the U.S. Government to ensure an open Internet. Assistant Secretary Lawrence Strickling, recently stated:

The multistakeholder process does not guarantee that everyone will be satisfied with the outcome. But it is critical to preserving the model of Internet governance that has been so successful to date that all parties respect and work through the process and accept the outcome once a decision is reached. **When parties ask us to overturn the outcomes of these processes, no matter how well-intentioned the request, they are providing “ammunition” to other countries who attempt to justify their unilateral actions to deny their citizens the free flow of information on the Internet. This we will not do. There is too much at stake here.** [Emphasis added.]⁸

⁸ Remarks of Assistant Secretary Strickling at the Practising Law Institute's 29th Annual Telecommunications Policy & Regulation Conference, December 8, 2011, available at <http://www.ntia.doc.gov/speechtestimony/2011/remarks-assistant-secretary-strickling-practising-law-institutes-29th-annual-te>.

**Senator Mark Warner
Commerce, Science, and Transportation Committee
Questions for the Record
“ICANN’s Expansion of Top Level Domain Names”
December 8, 2011**

Questions for Mr. Kurt Pritz

1. I understand the reasoning behind the high price of a new top level domain. It is important to me that the new gTLDs are only available to legitimate and serious organizations. However, up to 1,000 new TLD names at \$185,000 a piece is a considerable increase in income for ICANN. How will this money be used to regulate the expansive space new gTLDs will create? What are your plans for excess revenue? Will ICANN retain any revenue from the creation of new gTLDs? If so, how much revenue do you anticipate ICANN will receive over the next five years?

Answer to Question 1

ICANN shares your concern that a high bar is created to apply for a new gTLD, to help assure that new gTLDs are available to organizations that are serious in commitment to operate a portion of the Internet infrastructure. As discussed in response to Senator Cantwell’s Question 3, the New gTLD Program fee is operated on a cost-recovery basis. As provided to Senator Cantwell:

The \$185,000 application fee is calculated on a cost-recovery model, and was determined through a comprehensive and complex process that included identifying over 100 separate tasks required for the evaluation of a new gTLD application and seeking guidance from experts. The fee includes development costs (\$26,950 per application); application processing and evaluation costs (\$97,800 per application); and costs for expected contingencies, including allowance for unanticipated costs and variations between estimates and actual costs incurred (\$60,000 per application). A 14-page document setting out the methodology and further breakdown of the fee component is available at <http://www.icann.org/en/topics/new-gtlds/cost-considerations-04oct09-en.pdf>. This document is an update to the earlier “Cost Considerations of the New gTLD Program”, published in October 2008, available at <http://www.icann.org/en/topics/new-gtlds/cost-considerations-23oct08-en.pdf>.

While there is a possibility that multiple applicants for the same TLD could proceed to an auction to operate the TLD, ICANN intends the auction process as a last-resort method. ICANN encourages applicants to work together to arrive at a mutually-agreeable solution instead of allowing the competing applications to proceed to an auction. To the extent that a TLD proceeds to auction and generates additional funds, I discuss below ICANN’s commitments to using these funds towards its not-for-profit mission.

As a Not-for-Profit Public Benefit Corporation, ICANN is committed to its not-for-profit mission. For ICANN, that commitment requires us to assure that excess funds generated through the New gTLD Program (i.e., those that exceed the costs incurred for the processing, evaluation and other components of the New gTLD Program) are used in furtherance of ICANN's mission. The evaluation fee has been calculated to recover costs and not exceed those costs. If evaluation fees exceed actual costs, future evaluation fees will be reduced. If costs exceed fees, then ICANN will absorb that and future fees will be increased to meet the actual costs. For additional funds accruing to ICANN other than evaluation fees, such as the auction proceeds mentioned, the *Applicant Guidebook* addresses the issue in this way:⁹

It is planned that costs of the new gTLD program will offset by fees, so any funds coming from a last resort contention resolution mechanism such as auctions would result (after paying for the auction process) in additional funding. Any proceeds from auctions will be reserved and earmarked until the uses of funds are determined. Funds must be used in a manner that supports directly ICANN's Mission and Core Values and also allows ICANN to maintain its not for profit status.

Possible uses of auction funds include formation of a foundation with a clear mission and a transparent way to allocate funds to projects that are of interest to the greater Internet community, such as grants to support new gTLD applications or registry operators from communities in subsequent gTLD rounds, the creation of an ICANN-administered/community-based fund for specific projects for the benefit of the Internet community, the creation of a registry continuity fund for the protection of registrants (ensuring that funds would be in place to support the operation of a gTLD registry until a successor could be found), or establishment of a security fund to expand use of secure protocols, conduct research, and support standards development organizations in accordance with ICANN's security and stability mission.

In addition to evaluation fees, each registry will contribute \$25,000 annually to ICANN operations, policy development and community outreach activities. (If some registries become very large, they will pay greater fees.) That fee will cover contractual compliance, registry and IANA services for that registry, as well as contribute to the general ICANN activities described here. It has been urged by the community that ICANN "staff-up" to meet compliance, IANA function and other needs to adequately serve the new environment. If these revenues exceed needs, fees will be reduced.

ICANN handles its budgeting processes in an open and transparent manner. Not only will the community discussion regarding the use of funds be the subject of community

⁹ See Module 4, Page 19 of the *Applicant Guidebook*, version 2010-01-11.

consultation, but the funds will also be tracked and accounted for within ICANN's publicly-posted financial documents.

2. Federal Trade Commission Chairman Leibowitz recently stated that "a rapid, exponential expansion of generic TLDs has the potential to magnify both the abuse of the domain name system and the corresponding challenges we encounter in tracking down Internet fraudsters." His statement echoes the concerns of many that this expansion may be necessary, but the expansion from 21 gTLDs to up to 1000 gTLDs sounds extreme.
 - a. Why did ICANN choose to go from twenty-one top level domains up to over 500 in the first wave, or 1000 overall, instead of a more gradual increase over a set period of years? Can you please explain why this particular expansion program is the best plan for industry and consumers?

Answer to Question 2

The domain name system (DNS) today includes over 300 TLDs: 249 ccTLDs, 30 IDN ccTLDs, and 21 gTLDs. None of those 300 existing TLDs are required to include the standard protections that new TLDs must offer. The protections of the New gTLD Program were formed through ICANN's multi-stakeholder model.

ICANN has operated three pilot programs on the introduction of new TLDs into the DNS. In 2000, ICANN launched a "Proof of Concept" round, through which seven new TLDs were selected out of 44 applicants (proposing over 200 different potential TLDs). In 2004, ICANN accepted applications for Sponsored Top-Level Domains (sTLDs), specialized TLDs that are tied to defined sponsor communities (such as .CAT for the Catalan-speaking community). Finally, ICANN launched the IDN ccTLD Fast Track process in 2009 that, to date had resulted in the delegation of 30 IDN TLDs.

Through these pilot rounds, important lessons were learned. First, new TLDs can safely be added to the DNS. Second, the imposition of artificial restrictions on the rounds, such as the numerical restriction imposed in 2000 and the type-restriction imposed in 2004 place ICANN in the position of picking winners and losers, as opposed to fulfilling its mission of facilitating competition in the DNS. Artificial restrictions also create incentives for applicants to work to fit their TLD ideas into categories that may not be a true fit. The outcomes of the pilot rounds also helped inform the heightened protections in place for the New gTLD Program.

The gTLDs approved under this program will be introduced in a measured, limited manner. Rather than limiting by number or type, the round is limited by a high bar of required competencies and protections, and a limited application period. There is a 90-day application window, followed by a stringent evaluation process through which ICANN's expert evaluation panels will evaluate registry abilities to meet the high technical and operational requirements. The rollout of new gTLDs will be distributed over time – no TLDs are expected to be operational prior to early 2013; delegations of additional TLDs will be distributed after that, as the applications pass through the evaluation and dispute

resolution processes. The imposition of otherwise artificial limitations on today's New gTLD Program would only create incentives for the bad-acting applicants to seek advantages in a subjective evaluation process. The Program in place today allows applicants to be evaluated against objective standards.

As part of the consensus-building process, ICANN has agreed with governments and trademark holders that the next round of new TLD applications should occur after studying the impact of this round 's delegations on root zone stability and conducting a study on whether new trademark protections should be adjusted. ICANN will undertake these studies as soon as is practicable, in consultation with stakeholders. ICANN will also provide public updates on the ongoing process to determine the timing of the next round.

ICANN is also mindful of its commitment in the Affirmation of Commitments to, "organize a review that will examine the extent to which the introduction or expansion of gTLDs has promoted competition, consumer trust and consumer choice, as well as effectiveness of (a) the application and evaluation process, and (b) safeguards put in place to mitigate issues involved in the introduction or expansion."¹⁰

As discussed previously, the New gTLD Program today is created through over six years of policy and implementation work. The policy recommendations to guide the introduction of new gTLDs were created by the ICANN's Generic Names Supporting Organization (GNSO) over a two-year effort through its bottom-up, multi-stakeholder policy development process. The GNSO Council is comprised of all facets of the Internet community: Intellectual Property interests; business and commercial users; ISPs; non-commercial institutions, and ICANN's contracted registries and registrars.

In 2005, the GNSO initiated a formal, Bylaws-defined policy development process on the addition of new gTLDs. Policy recommendations are formed through consensus building among stakeholder groups representing: intellectual property, business, non-commercial interest, Internet service providers, registries and registrars. In the case of this program and the release of gTLDs in this manner, the GNSO approved the policy recommendations in 2007 by a bylaw described 19-1 vote in favor of the new gTLD Policy (the lone dissenting vote by a non-commercial interest found that the approved model had *too many restrictions*). The policy recommendations were submitted to ICANN's Board of Directors. In 2008, the ICANN Board approved the recommendations¹¹ and directed ICANN staff to commence the implementation phase.

After the directive to implement, ICANN continued working with the community on the design of the New gTLD Program to meet the policy recommendations. Since 2008, the

¹⁰ See <http://www.icann.org/en/documents/affirmation-of-commitments-30sep09-en.htm>.

¹¹ GNSO Final Report on the Introduction of New Top Level Domains ("Final Report"), at <http://gnso.icann.org/issues/new-gtlds/pdp-dec05-fr-parta-08aug07.htm> (Aug. 8, 2007); ICANN Board resolution, <http://www.icann.org/en/minutes/resolutions-26jun08.htm> (June 26, 2008); GNSO Minutes, <http://gnso.icann.org/meetings/minutes-gnso-29oct03.html> (Oct. 29, 2003).

Also see The GAC Principles Regarding New gTLDs, at http://gac.icann.org/system/files/gTLD_principles_0.pdf (Mar. 28, 2007).

New gTLD Program has been refined through ten independent expert working groups, 59 explanatory memoranda and independent reports, thousands of comments in no fewer than 47 extended public comment periods, and 1400 pages of comment summary and analysis. All comments were listened to and taken into account across eight versions of the *Applicant Guidebook*. The *Applicant Guidebook* implements the consensus policies developed by ICANN's multi-stakeholder community.

3. Cyber-crime is a growing threat to the security and stability of the Internet, with broad and direct public policy and financial impacts. Law enforcement agencies, which have experience combating cyber-crime, have identified a series of specific problems which are limiting their ability to address this growing threat. In 2009, these law enforcement agencies made 12 concrete recommendations to reduce the risk of criminal abuse of the domain name system. It is my understanding that none of the recommendations offered by law enforcement were included in the gTLD expansion program.
 - a. Can you please explain why ICANN chose not to include these recommendations?
 - b. How will ICANN cooperate with law enforcement moving forward to make sure that safety concerns are properly addressed?
 - c. How does ICANN plan to review applications from state-owned enterprises?
 - d. If problems develop in any of the new gTLDs, how will ICANN be able to adequately monitor and police any abuses or mismanagement?

Answer to Question 3

Law Enforcement Recommendations are Being Addressed

As mentioned in response to Senator's Cantwell's Question 2, ICANN is actively working to address all twelve of the law enforcement recommendations referenced in the GAC's October 27, 2011 communication. Specifically, as directed by the Board, ICANN is currently in negotiations with its accredited registrars on amending the Registrar Accreditation Agreement (RAA) to meet the recommendations raised by law enforcement authorities. Amendments are expected to be in force prior to the entry of the first new TLD in 2013.

These negotiations include face-to-face meetings with law enforcement agencies to ensure understanding of law enforcement requirements. The negotiation anticipates substantial and unprecedented steps to improve the accuracy of Whois data. ICANN is taking a strong stand in regard to issues relating to the verification of Whois data and expects the accredited registrars to take action to address the demands of governments and law enforcement worldwide. Updates on the negotiations are available at <https://community.icann.org/display/RAA/Negotiations+Between+ICANN+and+Registrars+to+Amend+the+Registrar+Accreditation+Agreement>.

By February 20, 2012, proposed amendments to address the law enforcement recommendations (and more) will be posted for public comment. One important aspect of the negotiations focuses on the verification of Whois data, and work is underway to plan a targeted forum, including representatives of law enforcement and experts in verification. This forum would be open to the public and is expected to take place before the ICANN meeting in Costa Rica.

Law Enforcement Helped Design New gTLD Protections

Addressing the 12 law enforcement recommendations for improvement to the gTLD *registrars* is just one part of how ICANN remains responsive to law enforcement. In fact, law enforcement agencies worldwide have worked closely with ICANN in the new gTLD implementation process, with a goal of reducing domain name abuses. Representatives of U.S. law enforcement agencies played a critical role in proposing standards for background screening for applicants. Law enforcement agencies worldwide, including the FBI, the UK Serious Organized Crimes Agency (SOCA) and the Royal Canadian Mounted Police, supported proposals to aid in the prevention and disruption of efforts to exploit domain name registration procedures for criminal purposes. ICANN has built a relationship with Interpol and discussed safeguards and, in particular, the implementation of meaningful background checks.

My testimony outlined a series of measures to mitigate against malicious conduct in new gTLDs, formed in part through law enforcement recommendation and involvement. Those measures include:

- Background reviews of TLD applicants, including reviews for criminal history (including the use of telecommunications or the Internet to facilitate crimes, illegal sale of drugs, and others);
- Rejection of applications where the applicant has a pattern of adverse decisions under the UDRP (Uniform Domain Name Dispute Resolution Policy), or has been found to act in bad faith or reckless disregard under cybersquatting legislation;
- The requirement to have a plan to implement domain name system security extensions (DNSSEC), reducing the risk of “man-in-the-middle” attacks and spoofed DNS records;
- A requirement to maintain enhanced, or “thick”, WHOIS records at the registry level to allow more rapid search capabilities, facilitating efficient resolution of malicious conduct activities;
- A centralized zone file access system to allow for more accurate and rapid identification of key points of contact within each gTLD. This reduces the time necessary to take corrective action within TLDs experiencing malicious activity;
- A requirement to establish a single point of contact responsible for the handling of abuse complaints (as requested by law enforcement authorities);

- Requirements that New gTLD Registry Operators must:
 - Maintain a Continued Operations Instrument sufficient to fund basic registry operations for a period of three years in case of business failure, to protect consumers and registrants within that gTLD in the event of registry failure.
 - Maintain continuity and transition plans, including regular failover testing.
 - Cooperate with ICANN In the event transition to a new registry operator is necessary. ICANN will identify an Emergency Back-End Registry Operator to assist in the registry transition process and provide emergency registry services as needed.

DNS abuse and security are regularly the subject of collaborative meetings between ICANN and the US law enforcement community, as well as representatives of international agencies.¹² ICANN expects this successful collaboration to continue. To that end, there are formal “DNS Abuse” sessions at every ICANN public meeting where ICANN and law enforcement representatives come together to advance this important work.

Applications from State-Owned Enterprises

All applications under the New gTLD Program are subject to the same application and evaluation process as laid out in the *Applicant Guidebook*. As part of the application process, ICANN acts in compliance with all U.S. laws, rules and regulation. This includes the economic and trade sanctions program administered by the Office of Foreign Assets Control (OFAC) of the U.S. Department of the Treasury. ICANN is prohibited from providing most goods or services to residents of sanctioned countries or their governmental entities or to specially designated nationals and blocked person without an applicable U.S. government authorization or exemption. ICANN generally will not seek a license to provide services (through the gTLD Program or elsewhere) to an individual or entity on the SDN list.

ICANN Commits to Continued Monitoring of New gTLDs

In response to your Question 1, we identify the reviews that ICANN has committed to undertake to assist in identifying the results of this first round. In addition to these reviews, ICANN is committed to a continued monitoring of the effects of the measured rollout of new TLDs, as well as working with law enforcement and the Internet community as a whole to identify new areas of concern and to be proactive in determining how to address new issues as they arise.

4. There are a number of failed top-level domain names from previous ICANN expansions – “.museum” for instance. Unfortunately, such failures can be costly for companies that have registered and they can be disruptive to users. Further, I

¹² ICANN’s relationships with law enforcement are not limited to the New gTLD Program; ICANN coordinates regularly on security-related issues and to address threats to the DNS.

understand that ICANN's own reports indicate that "if a new gTLD failed and ceased operation, external costs might be imposed on the Internet community. Registrants ... might be stranded....Internet users might face increased clutter on the Internet if links fail to resolve."

- a. The high-tech companies in Virginia– not to mention Internet users generally – would not welcome such volatility. What, if anything, has been done to address this concern?

Answer to Question 4

While the .museum registry may not have achieved a level of desired success or adoption, the .museum registry is still operational. No gTLD registries have failed during ICANN's existence. However, the risk of potential failure for a new gTLD registry is an understandable and valid concern. Among other safeguards, ICANN has in place provision for an "Emergency Back End Registry Provider" to take over operations for a failed registry to ensure the interests of registrants are protected and domain names continue to resolve.

The issue of registry failure has been considered in detail through the work on the New gTLD Program. First, the extensive evaluation process will help assure that only companies that meet the stringent financial requirements are able to operate new TLDs. Of course, this pre-emptive evaluation process may not fully protect against future registry failure, and ICANN has included multiple additional protections within the New gTLD Program to address potential failure.

During the application process, applicants are required to provide evidence that critical functions of the registry will continue to be performed even if the registry fails. This includes a requirement that the costs for maintaining critical registry functions over an extended period of time (between three to five years) be estimated as part of the application process, and registries must have available a Continuing Operations Instrument (funded through a letter of credit or an escrow account) that ICANN may invoke to pay a third party to maintain the critical registry functions.

ICANN is currently working to identify the entity that will serve as an Emergency Back End Registry Operator (EBERO), which will step in to perform the critical registry functions during the three-to-five year period. These provisions are expected to protect registrants against the risk of immediate registry failure.

To facilitate any need for emergency transition, ICANN also requires the escrow of registry data that the EBERO would be allowed to access for the purpose of providing the registry services.

In the event of a termination of a Registry Agreement, and in consultation with the registry operator, ICANN maintains the right to determine whether to transition the operation of a TLD to a successor registry operator as is necessary to protect the public interest. Transition is not required, however, if a registry operator's use of the TLD is for its own

exclusive use and all names are registered and maintained by the registry operator.

5. The protection and development of intellectual property is essential to economic growth in technology, and especially important to high-tech entities in Virginia. I am told that ICANN's own experts have said the following: "There may also be indirect harm from the loss of intellectual property owners' incentives to invest in that intellectual property due to concerns that some of the benefits of that investment would be misappropriated."
 - a. Is this an accurate statement?
 - b. Has anything been done to address this issue? If not, why is this expansion going forward in the face of such risks?

Answer to Question 5

Prior to this rollout, ICANN commissioned five economic studies that examined anticipated benefits and costs of the new gTLD program, the effects of price constraints, and the benefits of vertical integration. All support a conclusion that Internet users stand to benefit from the introduction of new gTLDs and that potential costs should be mitigated with the introduction of new safeguards.

As part of this work, economists did note that one of the potential external costs that may be imposed through new gTLDs is the impact on investments in intellectual property. However, in the same report, the economists clarified that these external costs can be reduced through the institution of "rules and procedure to protect companies' intellectual property rights." The economists noted that there are a range of effective rights protection mechanisms that balance intellectual property protections against the interests of those with legitimate interests in registering a domain name, including watch lists and sunrise periods. This is discussed in Michael Katz, Gregory Rosston and Theresa Sullivan's report entitled *Economic Considerations in the Expansion of Generic Top-Level Domain Names – Phase II Report: Case Studies*, available at <http://www.icann.org/en/topics/new-gtlds/phase-two-economic-considerations-03dec10-en.pdf>.

ICANN, with experts from the intellectual property community, addressed this cost/benefit concern. Trademark experts created rights protection mechanisms that exceed the bar suggested by the economists. The new trademark protection that help protect intellectual property rights and combat abuses include:

- Uniform Rapid Suspension: A rapid, inexpensive way to take down infringing domain names;
- Trademark Clearinghouse: a one-stop shop so that trademark holders can protect their property right in ALL new TLDs with one registration;

- Mandatory sunrise *and* Trademark Claims processes for *all* new gTLDs;
- The requirement to maintain thick Whois information, provision of centralized access to zone data, and a strong incentive to provide a searchable Whois database – all to make it easier to find infringing parties; and
- A post-delegation dispute procedure where rights holders can assert claims directly against TLD registry operators for domain name abuse if the registry has played an active role.

The implementation work to create the New gTLD Program carefully identified risks such as the one raised in your question, and created expert-informed solutions to address those risks. The Katz/Rosston report is just one of five economic studies performed in consideration of the New gTLD Program. All supported a conclusion that Internet users stand to benefit from the introduction of new gTLDs.

The four additional reports are:

- Dr. Dennis Carlton, Report Regarding ICANN’s Proposed Mechanism for Introducing New gTLDs, at <http://www.icann.org/en/topics/new-gtlds/carlton-re-proposed-mechanism-05jun09-en.pdf> (“Carlton I”);
- Dr. Dennis Carlton, Preliminary Analysis Regarding Price Caps for New gTLD Internet Registries, at <http://www.icann.org/en/topics/new-gtlds/prelim-report-registry-price-caps-04mar09-en.pdf> (“Carlton II”);
- CRA International, Revisiting Vertical Separation of Registries and Registrars, at <http://www.icann.org/en/topics/new-gtld-crai-report-24oct08-en.pdf>;
- Michael Katz, Gregory Rosston and Theresa Sullivan, An Economic Framework for the Analysis of the Expansion of Generic Top-Level Domain Names, at <http://www.icann.org/en/topics/new-gtlds/economic-analysis-of-new-gtlds-16jun10-en.pdf> (“Katz/Rosston Phase I”); and

The reports are detailed. Briefly summarized, the reports indicate that: benefits will accrue from the opening of this market in a way similar to other markets; innovation (and thus benefit) is difficult / impossible to quantify; and costs should be mitigated through the adoption of new trademark and consumer protections.

This work followed the careful consideration of the Internet community through ICANN’s bottom-up process.

Given the scope of the economic study already undertaken, as well as the commitment to measuring the effects of new gTLDs once there is actual data to inform that assessment, the Board and the Governmental Advisory Committee agree that further economic study would not be beneficial prior to the opening of the application round. Instead, the Board and the GAC focused on the collection of information that will inform the analysis of the effects of

the introduction of new gTLDs after this first round. The *Applicant Guidebook* now includes application questions that are specifically targeted to collect information relating to stated purposes and anticipated outcomes of each application, for use in later studies.

6. I've heard a number of questions from industry regarding their concerns with the new TLD system. However, these changes will also impact Internet users. I am concerned that some of my constituents will be confused by the new TLD program at the least and could be exposed to additional consumer harm such as cybersquatting, typosquatting, phishing, malware, etc. If it is more difficult for Internet users to determine whether a website is legitimate, it will be easier for criminals to lure Internet users to fake websites that include malicious content.
 - a. Can you please explain how the new program will change the internet for consumers?
 - b. How will ICANN work to make sure users are aware a coming changes and know how to navigate the new landscape?

What specific safeguards will be put into place to prevent cybersquatting and typosquatting?

Answer to Question 6

The protections within the New gTLD Program will create TLDs that are more secure for Internet users. For example, all new TLDs are required to implement domain name security extensions (DNSSEC), reducing the risk of “man-in-the-middle” attacks and spoofed DNS records. In terms of user confusion as a result of cybersquatting, the new protections for intellectual property and to mitigate malicious conduct all work to reduce cybersquatting activities in the expanded space. We expect that new TLDs will be a less fertile ground for wrongdoing and, as a result, the Domain Name System, as a whole will be improved. Abuses are prevalent in the larger TLDs, not within the smaller, more differentiated registries.

While there is always some uncertainty and concern with change, Internet users have always proved adept at adapting to change and taking advantage of new, value-added services. In the case of new gTLDs, it is thought that the new landscape will reduce confusion. TLDs that are clearly tied to brands or communities will create consumer awareness and result in more certainty. Also, that brand awareness will build certainty that a domain is what it purports to be – that is, reduce the risks of cybersquatting. As an example, take senate.gov names: users have great certainty that use of a .gov name will reliably lead to a U.S. Government site.

The New gTLD Program allows for community-based TLDs, as well as other TLDs that will have special attributes that may make them attractive to users. For example, work has been conducted towards creating a higher security TLD for the financial services industry, where the registry operator would commit to additional protections for the development of

a TLD where consumers know they are making financial transactions in a trusted space. The opportunities that may be available in new gTLDs are endless – the opening of the new gTLD space will allow for creativity and innovation that follows the opening of other markets.

ICANN and the Internet community recognize that there will be a need to educate consumers about the changing landscape of the Internet, and ICANN understands that communication and education is a necessary component of any rollout. ICANN is working with its stakeholder community to plan for this educational work.

**Senator Olympia Snowe
Commerce, Science, and Transportation Committee
Questions for the Record
“ICANN’s Expansion of Top Level Domain Names”
December 8, 2011**

Question for all witnesses

United Nations Model

There has been a growing contingency of other countries critical of the ICANN multi-stakeholder model and about the US’ involvement and influence with ICANN. Some governments, not necessarily friendly to the U.S., are seeking to increase their power over the Internet and its governance.

Russia and China (with Tajikistan and Uzbekistan) have proposed to the United Nations an Internet “Code of Conduct,” which a senior State Department official stated “they seek to justify the establishment of sovereign government control over Internet resources and over freedom of expression in order to maintain the security of their state.¹³” Even Russian Prime Minister Vladimir Putin remarked recently his desire of “establishing international control over the Internet using the monitoring and supervisory capabilities of the International Telecommunication Union (ITU).¹⁴”

The other proposal by India, Brazil and South Africa calls for the creation of a new body within the United Nations to oversee Internet policy. As a result, ICANN as well as the Internet Governance Forum (IGF) could be significantly marginalized or hijacked by this new UN entity.

These proposals seem to be in direct conflict with our nation’s effort to privatize the Internet through transferring the authority of the DNS to the private sector and for the Internet governance model to be private-sector led.

Question 1

If the US Government followed the advice to unilaterally delay the gTLD expansion, what do you believe the impact would be globally and do you believe this would fan the flames of anti-U.S. government sentiment with respect to Internet governance? Could it give more momentum to other governments’ calls to have the United Nations assert oversight over ICANN or replace it altogether?

Answer to Question 1

If the US Government or any entity unilaterally modified a decision by ICANN’s multistakeholder community, it would undermine if not decimate the legitimacy and credibility of the multistakeholder model. Lawrence Strickling, Assistant Secretary of Commerce for Communications and Information, has spoken forcefully on two recent

¹³ http://www.huffingtonpost.com/2011/09/27/russia-china-internet-control_n_984223.html

¹⁴ <http://premier.gov.ru/eng/events/news/15601/>

occasions in support of the multistakeholder model and the danger presented by requests for the US Government to unilaterally modify the new gTLD program. On December 8, 2011,¹⁵ he addressed these points as follows:

[W]e are now seeing parties that did not like the outcome of that multistakeholder process trying to collaterally attack the outcome and seek unilateral action by the U.S. government to overturn or delay the product of a six-year multistakeholder process that engaged folks from all over the world. **The multistakeholder process does not guarantee that everyone will be satisfied with the outcome. But it is critical to preserving the model of Internet governance that has been so successful to date that all parties respect and work through the process and accept the outcome once a decision is reached.** When parties ask us to overturn the outcomes of these processes, no matter how well intentioned the request, they are providing “ammunition” to other countries who attempt to justify their unilateral actions to deny their citizens the free flow of information on the Internet. This we will not do. There is too much at stake here. [Emphasis added.]

On January 11, 2012¹⁶ he stated:

[M]ultistakeholder processes have succeeded by their very nature of openness and inclusiveness. They are most capable of attacking issues with the speed and flexibility required in this rapidly changing Internet environment.

Nonetheless, we face challenges to this model even in our own country.

...

For the last six years, ICANN and its many stakeholders have debated the rules for expanding of the domain name system (DNS) – essentially the Internet’s address book -- through the introduction of new generic top-level domain names (gTLDs). ICANN’s process involved global stakeholders from the business community, civil society, registries, registrars, and governments. Nonetheless, in December we saw parties that did not like the outcome of that multistakeholder process trying to

¹⁵ Remarks of Assistant Secretary Strickling at the Practising Law Institute's 29th Annual Telecommunications Policy & Regulation Conference on December 8, 2011, (available at <http://www.ntia.doc.gov/speechtestimony/2011/remarks-assistant-secretary-strickling-practising-law-institutes-29th-annual-te>)

¹⁶ Remarks by Assistant Secretary Strickling at the Brookings Institution's Center for Technology Innovation, January 11, 2012 (available at <http://www.ntia.doc.gov/speechtestimony/2012/remarks-assistant-secretary-strickling-brookings-institutions-center-technology>).

bypass ICANN by seeking unilateral action by the U.S. government to overturn or delay the product of a six-year multistakeholder process that engaged folks from all over the world.

...

Each challenge to the multistakeholder model has implications for Internet governance throughout the world. When parties ask us to overturn the outcomes of these processes, no matter how well-intentioned the request, they are providing “ammunition” to other countries who would like to see governments take control of the Internet.

Question 2

If the U.N. did take control or governments had greater involvement, what impact would that have on American businesses and citizens that utilize the Internet? What impact could it have on Freedom of Speech?

Answer to Question 2

The Affirmation of Commitments between the U.S. Department of Commerce and ICANN sets out landmark commitments to “(a) ensure that decisions made related to the global technical coordination of the DNS are made in the public interest and are accountable and transparent; (b) preserve the security, stability and resiliency of the DNS; (c) promote competition, consumer trust, and consumer choice in the DNS marketplace; and (d) facilitate international participation in DNS technical coordination.”

Some of the commitments that ICANN undertakes include “commitments to: (a) maintain the capacity and ability to coordinate the Internet DNS at the overall level and to work for the maintenance of a single, interoperable Internet; (b) remain a not for profit corporation, headquartered in the United States of America with offices around the world to meet the needs of a global community; and (c) to operate as a multi-stakeholder, private sector led organization with input from the public, for whose benefit ICANN shall in all events act.”

While the ICANN model is not perfect, it has shown to be a powerful, dynamic model that is capable of reaching consensus positions on extremely difficult issues. The multistakeholder model that is ICANN is at risk if there is a heightened level of governmental involvement above that exercised today through the Governmental Advisory Committee (GAC). American businesses and citizens are very active in the ICANN model, and continuing to remain accountable to them – along with the global Internet community – is essential to ICANN’s mission.

Moving to a U.N. model pushes those stakeholders outside government to an inconsequential role. U.S. businesses would be reduced to influencing the U.S. vote in a one country – one vote model.

Assistant Secretary Strickling and former Ambassador David Gross have spoken eloquently on the negative impact of abandoning the multistakeholder approach to Internet governance issues. In the following excerpts, each describes proposals to give governmental bodies such as the UN's International Telecommunications Union (ITU) exclusive responsibility for Internet governance and standards development. Assistant Secretary Strickling recently described¹⁷ the proposals and their potential impact as follows:

Each challenge to the multistakeholder model has implications for Internet governance throughout the world.

...

As many of you are aware, this is precisely the challenge we face this December in Dubai, at the World Conference on International Telecommunications (WCIT). This conference, which is hosted by the International Telecommunication Union (ITU), attracts delegates from the ITU's 193 member countries.

...

[S]ome countries have submitted proposals to make ITU standards recommendations mandatory and thus enforceable by treaty, a drastic departure from their current voluntary nature. Some countries have proposed moving oversight of critical Internet resources into the ITU, including naming and numbering authority from multistakeholder institutions such as ICANN. Many governments have called for the ITU to play a greater role in regulating peering and termination charges in order to compensate for lost telecommunication fees, the so called "bypass phenomenon". Also, in an effort to establish the ITU as an operational authority on international cybersecurity, some more authoritarian countries have proposed to include cybersecurity and cybercrime provisions into the ITRs.

...

The challenge before us is clear. We must continue to make the case that an Internet guided by the open and inclusive processes as articulated in the OECD Policymaking Principles will encourage the rapid economic growth and wealth creation that the Internet has made possible.

It is incumbent upon us to convince other nations that enshrining the Internet in an international treaty will not accomplish these goals. The framework simply will not fit. An Internet constrained by an international treaty will stifle the innovators and entrepreneurs who are responsible for its awesome growth. As FCC Commissioner Robert McDowell recently said, "upending the fundamentals of the multistakeholder model is likely to Balkanize the Internet at best, suffocate it at worst". The states

¹⁷ *Id.*

who seek to impose their control over the Internet will only be further removed from its awesome potential.

Former Ambassador David Gross described¹⁸ the proposals and their potential impact as follows:

Once again, many companies in the telecoms and information and communications technology (ICT) sector are facing the spectre of a United Nations agency (in this case the International Telecommunication Union (ITU)) regulating critically important aspects of the internet as well as substantially expanding its jurisdiction over the telecoms and ICT industries.

...

Some within the ITU and among its 193 member states would like to see major changes to the treaty, particularly with respect to the internet as well as wireless, IP-based, and next-generation networks, which have historically been mostly free of intrusive economic and other regulation.

...

The WCIT could lead to new regulations governing how these businesses are run and how such businesses may interact with their customers, partners, and vendors, as well as how they can innovate and provide new and improved services. Moreover, because of the implicit attacks on established mechanisms of internet governance, the WCIT has the potential to destabilise and politicise standardisation processes and the management of the internet architecture in a way that could also hinder innovation and efficiency.

Question for witnesses

Growth of the Internet and expansion of the domain name system

The Internet has been so amazingly beneficial to small businesses because it allows them to globally expand their local markets and enables them to compete with Fortune 100 companies because the size of the computer screen is the same for a small business in Bangor as it is for a multi-national corporation like Wall-mart. Small businesses are the anchor to not only Maine's economy but to our nation's and the Internet has been invaluable to them.

¹⁸ "The 2012 World Conference On International Telecommunications: Another Brewing Storm Over Potential UN Regulation Of The Internet," November 2011 (available at <http://www.whoswholegal.com/news/features/article/29378/the-2012-world-conference-international-telecommunications-brewing-storm-potential-un-regulation-internet/>). See also, "Governments vie for control of the Web," by Eliza Krigman, POLITICO Pro, January 18, 2012 (available at <https://www.politicopro.com/story/tech/?id=8499>; subscription required)("The end result [of adoption of some proposals at the WCIT], American officials warn, would be an Internet more susceptible to censorship and less potent as a tool to foster democracy.")

Supporters of the expansion have stated it will bring new competition and choice to the Internet space and allow the Internet to continue to grow in the number of websites, content, applications, and online services. It also presents businesses new models to harness the boundless benefits of the Internet.

There have already been expansions to top level domains in the past to accommodate for the growth of the Internet, with the intro of gTLDs like .biz, .info, .museum, .mobi, etc.

Question 3 (For all witnesses)

If the Internet is going to continue to grow shouldn't the domain name system?

Answer to Question 3

Yes. Since 1998, ICANN has been working to execute on its promise to facilitate competition in the Domain Name System while protecting vital security, consumer and business interests. The New gTLD Program has been carefully crafted over the past six years to achieve this goal. As stated in my written testimony,

A founding mandate for ICANN, included within the United States Government's "White Paper on the Management of Internet Domain Names and Addresses",¹⁹ is to create competition in the domain name market and specifically, to "oversee policy for determining the circumstances under which new TLDs are added to the root system."²⁰ The introduction of new gTLDs "has been a longstanding goal" of the relationship between the Department of Commerce and ICANN.²¹ The relationship formed with the United States Government in 1998, and set out in the many Memoranda of Understanding between the Department of Commerce and ICANN, included a core objective to "Define and implement a predictable strategy for selecting new TLDs."²² This fundamental assumption that increasing the number of gTLDs will increase competition resulted in the House Committee on Energy and Commerce

¹⁹ United States Department of Commerce, *White Paper on the Management of Internet Domain Names and Addresses* ("White Paper"), at http://www.ntia.doc.gov/ntiahome/domainname/6_5_98dns.htm (June 6, 1998)

²⁰ *Id.*

²¹ Testimony of Fiona Alexander, Associate Administrator, National Telecommunications and Information Administration, June 4, 2009, before the Subcommittee on Communications, Technology, and the Internet, Committee on Energy and Commerce, United States House of Representatives, available at <http://www.ntia.doc.gov/speechtestimony/2009/testimony-associate-administrator-fiona-alexander-issues-concerning-internet-co>.

²² *See, e.g.*, Amendment 6 to Memorandum of Understanding Between the U.S. Department of Commerce and The Internet Corporation For Assigned Names And Numbers, at http://www.ntia.doc.gov/ntiahome/domainname/agreements/amendment6_09162003.htm (Sept. 16, 2003).

initiating a 2001 hearing regarding the potential detrimental effects to competition when ICANN approved only seven of 200 applied-for TLDs in an earlier application round.²³

Today, the DNS is continues to grow. The next billion Internet users will be from outside the U.S. but their participation represents opportunity for all businesses and communities. Since 2010, 30 new country code top-level domains in non-Latin scripts have been added to the DNS. These internationalized domain names, or IDN ccTLDs, help bring the Internet to the next billion people. We've seen innovation in the business models for existing country code TLDs, such as .CO (Colombia) and .ME (Macedonia) to take advantage of commercial opportunities waiting in the U.S. and beyond. But only TLDs introduced under the New gTLD Program will provide the significant, mandatory protections I describe in my testimony. The introduction of the New gTLD Program is therefore not just fulfilling a mandate to add competition through the introduction of more TLDs, but also represents the creation of a new, more secure baseline for the expansion of the Domain Name System.

Question for witnesses

White Paper

In the "White Paper," which was released in 1998 and led to the formation of ICANN is competition, has as one of its core principles is competition—that competition and consumer choice should drive the management of the Internet because they will lower costs, promote innovation, encourage diversity, and enhance user choice and satisfaction.

Comments in the White Paper²⁴ on the issue of new generic top level domains showed "very strong support for limiting government involvement during the transition period on the matter of adding new gTLDs. Specifically, most commenters -- both U.S. and non-U.S.-- suggested that it would be more appropriate for the new, globally representative, corporation to decide these issues once it is up and running." Also, commenters noted that "there are no artificial or arbitrary limits in other media on the number of places in which trademark holders must defend against dilution."

Question 1 (For all witnesses)

Isn't the expansion of gTLD a form of competition, where .hotels or .cars could compete against .com or .biz? If not, why?

Answer to Question 1

²³ See Transcript of February 8, 2001 Hearing before the Subcommittee on Telecommunications and the Internet of the Committee on Energy and Commerce, House of Representatives, On Hundred Seventh Congress, First Session, *available at* <http://archives.energycommerce.house.gov/reparchives/107/hearings/02082001Hearing37/print.htm> ("some view ICANN's approval of only a limited number of names as thwarting competition").

²⁴ <http://www.ntia.doc.gov/federal-register-notice/1998/statement-policy-management-internet-names-and-addresses>

Yes. In response to your Question 3 under the “*Growth of the Internet and expansion of the domain name system*” heading, it is noted that the introduction of the New gTLD Program is expected to fulfill ICANN’s mandate to introduce competition in the DNS. ICANN does not know all of the potential business models that are contemplated, nor is ICANN in a position to judge or foretell which business models may succeed. That is the role of the market. ICANN’s role is to allow for the creation of opportunities in the DNS for marketplace participants to compete, to innovate and to offer users new products and services.

For at least the past two years, future applicants have attended ICANN meetings, passing out marketing materials with their “dot-*NEWDOMAIN*” prominently displayed. Consulting businesses to advise applicants have arisen. Over 120 persons or entities have publicly announced their intention to apply for new gTLDs. Nearly 90 declared applicants have active websites marketing their new gTLD idea proposing all types of gTLDs – city names, community ideas, branding opportunities for internationally known corporations and others.

There are other forms of competition in addition to new gTLDs, for example, the introduction of services provided by Twitter and Facebook, and also the increased use of “apps.” However, one form of introducing competition should not foreclose another. The formation of ICANN in 1998 and the potential introduction of new gTLDs have been clearly described as an opportunity for increasing competition, choice and innovation. That introduction has taken place in a careful way, including two limited rounds in 2000 and 2004, the limited introduction of IDNs starting in 2010.

There is tremendous opportunity for innovation, competition and consumer choice within the New gTLD Program.

Question 3 (For all witnesses)

Several commenters also stated “the market will decide which TLDs succeed and which do not.” What is wrong with allowing the market to continue to decide with new gTLDs from the expansion?

Answer to Question 3

Allowing the market to determine the success of new gTLD offerings is one of the fundamental tenets of the introduction of the New gTLD Program. One of the policy recommendations that serves as the basis for this program is that the introduction of TLDs should only be limited by round, and not by subjective and arbitrary factors. In addition, the economic studies, described in response to Senator Warner’s Question 5, support that competition results from the opening of markets – not by imposing artificial limitations such as number or type.

One of those economists, Dr. Dennis Carlton, Deputy Assistant Attorney General for Economic Analysis, Antitrust Division, U.S. Department of Justice from October 2006 through January 2008, explained: “ICANN’s plan to introduce new gTLDs is likely to benefit

consumers by facilitating entry which would be expected both to bring new services to consumers and mitigate market power associated with .com and other major TLDs and to increase innovation.”²⁵ Delay will inhibit competition in the use of generic, non-trademarked terms, and runs counter to the generally accepted view that market entry benefits consumers by expanding output and lowering price. Potential innovations in the new gTLD namespace will be stifled if limitations to entry are imposed, which would “essentially freeze the number of TLDs fifteen years after the first commercial development of the Internet.”²⁶

The introduction of new gTLDs will also serve to alleviate issues in existing market conditions: concentration within some existing registries, most generic strings unavailable, and those that trade on the value of the current marketplace holding portfolios based upon the value of current .COM names.²⁷

While the market should decide which TLDs succeed and which do not, we understand the valid concerns associated with registry failure and ICANN has put into place consumer interest protections.

Among other safeguards, ICANN has in place provision for an “Emergency Back End Registry Provider” to take over operations for a failed registry to ensure the interests of registrants are protected and domain names continue to resolve.

The issue of registry failure has been considered in detail through the work on the New gTLD Program. First, the extensive evaluation process will help assure that only companies that meet the stringent financial requirements are able to operate new TLDs. Of course, this pre-emptive evaluation process may not fully protect against future registry failure, and ICANN has included multiple additional protections within the New gTLD Program to address potential failure.

During the application process, applicants are required to provide evidence that critical functions of the registry will continue to be performed even if the registry fails. This includes a requirement that the costs for maintaining critical registry functions over an extended period of time (between three to five years) be estimated as part of the application process, and registries must have available a Continuing Operations Instrument (funded through a letter of credit or an escrow account) that ICANN may invoke to pay a third party to maintain the critical registry functions.

ICANN is currently working to identify the entity that will serve as an Emergency Back End Registry Operator (EBERO), which will step in to perform the critical registry functions during the three-to-five year period. These provisions are expected to protect registrants against the risk of immediate registry failure.

25 Dr. Dennis Carlton, Report Regarding ICANN’s Proposed Mechanism for Introducing New gTLDs, at <http://www.icann.org/en/topics/new-gtlds/carlton-re-proposed-mechanism-05jun09-en.pdf> at paragraph 23.

26 *Id.*

27 Katz/Rosston Phase II, at paragraphs 75-76.

To facilitate any need for emergency transition, ICANN also requires the escrow of registry data that the EBERO would be allowed to access for the purpose of providing the registry services.

In the event of a termination of a Registry Agreement, and in consultation with the registry operator, ICANN maintains the right to determine whether to transition the operation of a TLD to a successor registry operator as is necessary to protect the public interest. Transition is not required, however, if a registry operator's use of the TLD is for its own exclusive use and all names are registered and maintained by the registry operator.

ICANN's past experience with its 2000 and 2004 pilot programs on the introduction of new gTLDs, described in response to Senator McCaskill's Question 2, represent limited expansion. ICANN learned valuable lessons from each of these rounds: First, new TLDs can safely be added to the DNS. Second, the imposition of artificial restrictions on the rounds, such as the numerical restriction imposed in 2000 and the type-restriction imposed in 2004 place ICANN in the position of picking winners and losers, as opposed to fulfilling its mission of facilitating competition in the DNS. Artificial restrictions also create incentives for applicants to work to fit their TLD ideas into categories that may not be a true fit.

Today's New gTLD Program instead allows for competition tempered by the suite of new protections for trademark owners and Internet users. Choice and competition will be introduced in a more secure environment than ever before.

Question 4 (For all witnesses)

If commenters are correct that "there are no artificial or arbitrary limits in other media on the number of places in which trademark holders must defend against dilution" then why should we place "artificial or arbitrary" limits on the Internet?

Answer to Question 4

Today's New gTLD Program is balanced so as not to impose artificial or arbitrary limits of any kind. Limits on the Program were created to safeguard specific, important interests, for example, property rights and community interests. The mandatory rights protection mechanisms in place for the New gTLD Program are broader than the protections offered to trademark holders in the rollout of any other media of which I am aware. However, the rights protection mechanisms were carefully crafted, balancing the input of trademark experts against third parties with legitimate rights to register domain names. To that end, including the suite of trademark protections in the New gTLD Program is not an "artificial or arbitrary" limit on the Internet and ICANN is committed to enforce the mandatory requirements. The creation of trademark protections is also supported by the economic analysis described in response to Senator Warner's Question 5.

The protections that exist are careful and balanced. Further, ICANN has agreed to undertake studies of a post-launch review on the feasibility of enhancing both the scope of the words registered within the Trademark Clearinghouse and the length of the Trademark Claims notification process. If further protection is warranted and feasible, these enhanced

protections could be included in future gTLD application rounds. Imposition of drastic limitations – and creating rights that are neither justified on the basis of experience nor recognized in other areas – could impair the ability for competition to flourish in new gTLDs.

Question for NTIA and ICANN witnesses

Expansion of Internet addresses

The Internet has revolutionized some many different areas of society and the economy. The innovation, adoption, and sheer size of the Internet are simply unparalleled. The Internet currently comprises of approximately 2 billion users and more than five billion devices. Cisco estimates there will be more than 50 billion internet connected devices by 2020.

However, we have for the most part exhausted the existing pool of Internet address— IPv4 provides for approximately 4.3 billion addresses. The shortage has been the driving factor in creating and adopting several new technologies as well as new and larger addressing system, known as IP version 6. This migration from a 32-bit addressing space to a 128-bit addressing, will provide 340 trillion, trillion, trillion separate addresses—enough for every human bring to use many trillions of address. With IPv6, there will be approximately 670,000 IP addresses for every squared nanometer of the earth's service. To put that into perspective, a human hair is 100,000 nanometers wide.

However, the implementation of IPv6 has been somewhat slow. Last year, I read only about 20 percent of the Internet was IPv6 compatible and while a recent survey shows adoption of IPv6 grew by 1,900 percent over the past 12 months that results in only about 25 percent of .com, .net, and .org Internet subdomains.

Question 1

What is the status of the migration to IPv6 and what will it mean for Internet users and businesses, domestic and globally?

Answer to Question 1

While universal IPv6 deployment is likely to obviate the need for IPv4 deployments in the long-term, the short and medium-term is likely to see Internet networks running both protocols side-by-side for years to come. As such, migration away from IPv4 is a less important goal than the widespread deployment of IPv6.

The status of IPv6 deployment can be measured both quantitatively and qualitatively. Quantitatively, over 7,500 IPv6 address blocks had been allocated to network operators around the globe by the end of September 2011²⁸ and by January 2012, the American Registry for Internet Numbers (ARIN) allocated IPv6 address blocks to over 2,300

²⁸ http://www.nro.net/wp-content/uploads/nro_stats_2011_q3.pdf

networks in the USA²⁹ alone. Almost 6,700³⁰ IPv6 networks were publicly routed on the Internet in January 2012, which is approximately 17%³¹ of Internet networks.

Qualitatively, IPv6 deployments have undergone testing and are now being made as part of ISPs and content providers' standard services. World IPv6 Day³² in June 2011 was a coordinated test of IPv6 by including Google, Facebook, Yahoo!, Akamai and Limelight Networks, together with over 1,000 web site operators. It was a success, and June 6, 2012 will see the World IPv6 Launch, in which major ISPs, home networking equipment manufacturers and web companies around the world are coming together to permanently enable IPv6 for their products and services.

While June's World IPv6 Launch is not a flag day, the combination of successful testing and market leading deployment is expected to provide an incentive to other Internet businesses and help raise awareness with non-Internet businesses. Some businesses may note that they need to update systems to allow for IPv6 deployment, though regular updating of systems to meet with technological advances is a normal cost of business. However, successful IPv6 deployment should be seamless for Internet users, whose computer operating systems have been IPv6 capable for some years already.

Question 2

Is there anything governments can do to encourage faster adoption of IPv6 as well as increase awareness to businesses and citizens about the migration?

Answer to Question 2

From ICANN's perspective, public support for adoption of IPv6 can help increase awareness of the deployment of IPv6, as well as provide incentives for Internet-related businesses to engineer products that are capable of IPv6 deployment. For example, in 2005, the United States Office of Management and Budget (OMB) mandated³³ that federal agencies initiate the transition to IPv6. The target readiness date was June 2008. In September 2010 the OMB released a further memorandum³⁴ setting out additional deadlines for the federal IPv6 transition. Other national governments have introduced similar roadmaps. Examples include Australia's 2009 Strategy for the Implementation of IPv6 in Australian Government Agencies³⁵ and the European Commission's Action Plan for the deployment of Internet Protocol version 6 (IPv6) in Europe.³⁶ The latter has guided

²⁹ <ftp://ftp.arin.net/pub/stats/arin/>

³⁰ <http://www.cidr-report.org/v6/as6447/index.html>

³¹ <http://www.cidr-report.org/as2.0/>

³² <http://www.worldipv6day.org/>

³³ http://www.cio.gov/documents/Transition_Planning_for_IPv6.pdf

³⁴ <http://www.cio.gov/Documents/IPv6MemoFINAL.pdf>

³⁵ http://www.finance.gov.au/e-government/infrastructure/docs/Endorsed_Strategy_for_the_Transition_to_IPv6_for_Australian_Government_agencies.pdf

³⁶

http://ec.europa.eu/information_society/policy/ipv6/docs/european_day/communication_final_27052008_en.pdf

deployment in governments throughout Europe, including Germany.³⁷

Mandates such as OMB's 2005 timeline have helped establish demand for IPv6 feature sets, as customers now require those features in equipment purchases. As such, governments have contributed to the success of World IPv6 Day in 2011, which readied the stage for this year's World IPv6 Launch.

³⁷ <http://ripe58.ripe.net/content/presentations/ipv6-in-germany.pdf>