To: ICANN (gtld-guide@icann.org)
Re: Industry Comments to the New GTLD Program and Process
Date: December 15, 2008

Dear Dr. Twomey and Mr. Dengate Thrush:

The undersigned corporations, trade associations and business groups, representing thousands of multi-national companies and millions of employees and Internet users, submit these comments related to the Draft Applicant Guidebook and the new generic Top Level Domain (gTLD) program.

Since the inception of the Internet, the global economy has thrived thanks to the World Wide Web's ability to bring businesses and consumers together to engage in eCommerce in a manner that is increasingly more safe and secure. The stability of the Internet as a global platform for eCommerce is a core concern for businesses world-wide, and we look forward to working with ICANN to ensure this stability, especially in these times of great economic uncertainty. We submit these comments to you in light of this commitment.

Executive Summary

ICANN's decision to increase the number of gTLDs has brought a number of issues to the attention of the international business community, and we would like to take this opportunity to address them. Most significantly, our concerns lie in three significant areas:
- Protecting consumers across the new gTLDs;
- Protecting brand-owners across the new gTLDs; and
- The effect of the new gTLD program on ICANN and the Internet.

Our comments below highlight these three areas. We suggest that before ICANN proceeds with the new gTLD Program and Process, it should:
- Undertake the full economic study of the domain name marketplace mandated by the ICANN Board in 2007, as well as an extensive evaluation of whether new gTLDs are needed in the first place given the record of existing new gTLDs;
- Establish criteria for success of new gTLDs in the proposed first round – including Internationalized Domain Name (IDN) TLDs – before moving forward;
- Modify the roll-out of the new gTLD program to only sponsored gTLDs and a limited number of IDN TLDs once the study has been completed and criteria established; and
- Limit further roll-out until sufficient safeguards are in place to protect Internet users, businesses, and brand-owners alike from any existing and expected acts of cyber-fraud.

Until these issues and recommendations can be adequately addressed, we respectfully request that ICANN delay the launch of the new gTLD program.

Protecting Consumer Across the New gTLDs

It can be said that the Internet exists for its users, as well as because of its users. Protecting them from harm is incredibly important not only for their sake, but also for the sake of all who create content, do business and facilitate the Internet's day-to-day operations on the network.

Preventing Consumer Confusion

ICANN has announced its intention to move forward with plans for creating a considerable number of new generic TLDs, including IDNs. One justification ICANN has noted for this is to introduce 'competition' into the domain name system (DNS).   Currently, there are over 240 top level registry strings (known as top level domains or TLDs) that include generic names (gTLDs) such as .com, .net; .info; .biz; .mobi; as well as country-code TLDs (ccTLDs), such as .us, .uk, .it, and .cn. Today, in these top level domains, over 175 million domain names already offer significant choice and diversity to end registrants. ICANN's proposed approach to introducing further new TLDs could lead to the creation of over 1,000 or more new gTLDs over the next three years. This course of action would significantly raise the risk of creating confusion in the minds of consumers as to where on the Internet they can find a business or their desired product. By making it increasingly difficult for consumers to enjoy their Internet experience, frustrated consumers would be less likely to engage in eCommerce – in a time when many businesses with online presences can ill afford reduced traffic.

Protecting consumers against cyber-fraud

With the increased number of gTLDs, the opportunity for cyber-crime to increase is significant. By using domain names to exploit the trust that consumers have in legitimate brands and trademarks, cyber-squatters are able to harm consumers through creating confusion about which web site is the legitimate brand-holders site that provide the goods or services the user is seeking. Other serious problems exist when these illegitimate sites are used for abusive purposes, such as sending malware to infect a user's computers with viruses and software to steal personal information, as well as through the sale of unwanted counterfeit goods.

The magnitude of the problem is shocking. The overall number of domain names under existing gTLDs has more than doubled since 2003, and the growth of cyber-squatting has exceeded that pace. According to MarkMonitor's Brandjacking Index Report from Spring 2007, cyber-squatting increased 248% in 2006.[1] This is of significant concern as cyber-squatting is a tool that criminals use in phishing attacks against unsuspecting consumers. A study released by Gartner, Inc. in 2007 revealed that phishing attacks in the United States alone cost Internet users over $3.2 billion.[2] The problem is growing, with no signs of slowing down. The survey found that 3.6 million adults lost money in phishing attacks in the 12 months ending in August 2007, as compared with 2.3 million the previous year.[3] With the projected number of new gTLDs created in the proposed program, the costs of fraud to unsuspecting consumers will undoubtedly eclipse that figure.

ICANN's efforts must include consideration of the millions of Internet users who use the World Wide Web to work, play and learn. Strong consumer protection starts with creating tools to thwart brand infringement, so as to protect against such potential and probable abuses in new gTLDs and in IDNs.

---

[1] MarkMonitor Brandjacking Index, Spring 2007. (See also:
http://www.markmonitor.com/download/bji/BrandjackingIndex-Spring07.pdf)
[2] Gartner, Inc. (December 17, 2007). "Gartner Survey Shows Phishing Attacks Escalated in 2007; More than $3 Billion Lost to These Attacks." Press Release. Retrieved on 11 December 2008. (See also:
https://www.gartner.com/it/page.jsp?id=565125).
[3] Ibid.

Protecting Brands Across the New gTLDs

There is great concern in the business community that ICANN has not adopted adequate safeguards against systemic brand abuse in new gTLD registrations (including both ASCII and non-ASCII (or IDN) TLDs) prior to moving forward with the new gTLD Program. The current system for addressing brand abuse is the Uniform Domain Name Dispute Resolution Policy (UDRP). Currently, there are almost 250 TLDs available to public, as well as to private and governmental institutions. Trademark owners are already compelled to engage in defensive registrations to prevent phishing, fraud, and trademark infringement.

As mentioned above, cyber-squatting is not only a problem that impacts consumers and business. The practice is estimated by the Coalition Against Domain Name Abuse to cost brand owners worldwide over $1 Billion dollars a year as a result of diverted traffic, the loss of hard-earned trust and goodwill, and the increasing enforcement expense of protecting consumers from Internet-based fraud. Adding new gTLDs without adding the proper tools to protect Internet users and brand owners will only exacerbate and already out-of-control problem.

In sum, the ICANN proposal would vastly increase the costs associated with defensive registrations and mark protection, which are already extremely expensive for trademark owners, even where there are only a finite number of TLDs. We believe that, by adopting the following recommendations, ICANN can strengthen the security and integrity of the DNS while simultaneously protecting consumers and brand-owners.

The current and future quality of the WHOIS system

Continued access to an accurate WHOIS is essential to protect the stability and security of the Internet, as well as to maintain confidence of consumers in the integrity and safety of eCommerce. Examples of essential characteristics of WHOIS:

- Free, accurate, and publicly available access to WHOIS, to quickly identify the registrant of abusive domain names, is critical to the future of the gTLD program;
- Applicants committed to maintaining and enforcing WHOIS requirements, including a centralized or "thick" WHOIS; and
- True applicant information in proxy registrations should be escrowed until the application is verified against an IP Registry. A mechanism that allows access to the data under the defined conditions should be developed and implemented in a uniform manner.

The application process for new gTLDs should require applicants to genuinely commit to participate in an open and accurate WHOIS system. Proxy and private registrations frustrate the efforts of trademark owners to identify domain name registrants and should be strongly discouraged, if not prohibited. The growth of online fraud and, in particular, phishing, necessitates stronger action at the registration level to ensure that criminals can be quickly identified and stopped. Even if applicants are not prohibited from anonymously registering domains, at a minimum trademark owners must be able to identify expeditiously the actual entity or individual responsible for registering a domain name that conflicts with one of their marks.

<u>Lack of tools for brand owners to protect their brands and their customers</u>

Currently, there are few options for brand owners, other than self-policing, use of the U.S. Anti-Cyber-Squatting Act, and the Uniform Domain Name Dispute Resolution Policy (UDRP) to protect their brands over the Internet. To promote the success of the proposed gTLD program, new tools and safeguards could be created by ICANN. Such mechanisms should be in place before the new TLD application window opens, and all registry applicants should be required to follow standardized processes.

One possibility includes a centralized registry of qualified names that would act as a clearing house for "certified" brand-holders, based on objective criteria. This no-cost "reserved list" would enable trademark owners to make sure that they can put their own names "on hold" without being forced to register in all these new places either during the so-called "sunrise period," which would be hugely expensive, or after. ICANN implicitly recognizes that additional costs that will be imposed on trademark owners because it creates a Top-Level Reserved Names List consisting exclusively of ICANN-related names. We believe that ICANN must offer the same solution to brand owners.

We note specifically that this list would not constitute a famous mark list but would be open to any trademark owner who could meet certain objective criteria. For instance, the trademark owner would need to establish that they own a national trademark registration in at least one of the five ICANN geographic regions. The trademark owner must also demonstrate through documentation that their marks have been the subject of widespread cybersquatting as established by successful UDRP proceedings or other proceedings brought in national courts of competent jurisdiction.

Once these hurdles have been met by a trademark owner, their name would be placed on the reserved list. A prospective applicant who wishes to register a name that is on the list would have their application automatically flagged, at which point the applicant can bring an expedited administrative proceeding to allow its name to move forward. This proceeding would be administered by the arbitration and mediation center of the World Intellectual Property Organization, which has already been identified by ICANN as a potential dispute resolution service provider (DRSP) and has established expertise in resolving trademark and domain name disputes.

In determining whether trademark rights are implicated, the use of algorithms (based solely on visual similarity) in and of themselves, are not a panacea for the protection of intellectual property rights. Algorithms alone cannot be dispositive of string similarity. There must be manual reviews to ensure adequate protection of marks. Visual, aural and semantic similarity should be emphasized in determining whether the registration of various domain names may be implicated.

Lastly, the UDRP process can be slow and cumbersome. Trademark owners may suffer harm before they can fully vindicate their rights in a UDRP dispute. Another tool that ICANN should consider are mandatory notice/take-down procedures for infringing second-level names based on established criteria in the new gTLDs, similar to the U.S. Digital Millennium Copyright Act.

<u>The cost of dispute resolution procedures</u>

Currently, utilizing the UDRP for brand protection is costly and time consuming; under the proposed gTLD Program, the UDRP as a remedy will be impractical and cost prohibitive with the possibility of dozens to hundreds of new gTLDs to police.

As far as brand protection in resolving string contention in the new gTLD application process, auctions should be avoided and other improved mechanisms for resolution should be developed. If there are cases in which an auction is necessary, bidders should be required to put into an escrow account an amount large enough to deter fraudulent or defaulting bidders. Further, the utilization of auctions and resultant revenues to ICANN need to be assessed regarding implications for affecting ICANN's non-profit status.

As mentioned above, given the number of expected TLDs in the first-round alone, the cost-potential for brand-holders to protect their brands is daunting. To help alleviate this burden in the UDRP process, prevailing brand-holders in a dispute should not experience any fees or costs in protecting their brand. This could be accomplished by extending the loser-pays approach of the dispute resolution process to cover all costs and expenses, including attorney fees as well as filing fees paid to the DRSP. This will result in a more fair and equitable dispute resolution process, with the added benefit of curbing registrations used for harassment purposes.

Strengthening the dispute resolution system

To promote the success of ICANN's proposed gTLD Program, it is critical that dispute resolution service providers' (DRSP) decisions should be final and binding on ICANN, rather than be viewed as an "expert determination" to be considered by ICANN as a factor in the evaluation of the gTLD application. Further, objections and responses should be made public. Lastly, objectors in dispute resolution proceedings should not be forced to give up all their legal rights, specifically including the right to seek redress in court.

The Effect of the New gTLD Program on ICANN and the Internet

Concern over the need for new gTLDs

Given the unease over the unintended consequences for Internet users and brand-holders alike, a significant question arises over whether or not new gTLDs are needed in the first place. ICANN's previous expansion of gTLDs has largely failed to increase the number of registrants that ostensibly justified the creation of new gTLDs. The .COOP, .AERO, .MUSEUM, and .JOBS gTLDs, for example, have no more than 10,000 registrations each. As of this date, there has been no evidence to suggest a compelling demand for the expansion of new TLDs. Prior to embarking on such a program as this, it would be advisable to study whether or not competition in the domain-name marketplace, as ICANN asserts, is actually lacking.

To that point, the ICANN Board directed its President more than two years ago to commission a comprehensive study on the economics of the domain registration marketplace.[4] However, this has not occurred. Such a study would be invaluable for crafting a new gTLD launch in a way that maximizes the competitive benefits. We strongly recommend the study should be started immediately and prior to moving forward with the new gTLD Program. If competition is found to be lacking, the next logical step would be to assess potential causes of the lack of competition, as well as address remedies and their impact on the Internet community as a whole.

---

[4] See http://www.icann.org/en/minutes/minutes-18oct06.htm.

Assessing the success of the new gTLD Program

Given the scope and size of the current undertaking, there should be significant delays in between application rounds to understand a number of issues critical to the health of the DNS, such as:

- Whether trademark owners will be able to vindicate their intellectual property rights given the introduction of any new gTLDs;
- Whether the costs associated with brand management and mark protection justify the benefits of the new gTLDs; and
- Whether the new gTLDs, in fact, do yield any tangible benefits to the broader Internet community.

The impact of new gTLD new revenue streams on ICANN's non-profit corporation status

The proposed new gTLD Program stands to increase ICANN's coffers significantly. Prior to issuing its 2007 annual report, ICANN maintained an $18 million balance. As a result of its revenue streams in 2007, ICANN now maintains a $35 million balance. There are serious concerns that ICANN is not fulfilling its charitable purposes under U.S. law by building up large reserves, far beyond the "Basic Cost Recovery Principle" set forth by ICANN ten years ago.[5]

Colleges and universities have recently been subject to increased scrutiny by the IRS and Congress for effectively hoarding their endowments at the expense of achieving the underlying missions that give rise to their tax-exempt status. To avoid any unwanted scrutiny, ICANN should not use the additional revenues it will gain as a result of this new gTLD system for any purpose other than the stated purposes in its Charter and Bylaws.

Industry strongly believes that with the new revenue streams created by new gTLDs, ICANN should commit to expending additional resources to ensure the security, stability and integrity of Internet commerce. Such measures should include establishing mechanisms to ensure that trademark holders have adequate and effective tools to protect their intellectual property rights.

Summary

In viewing the new gTLD Program in light of the existing system, observers have noted that ICANN may not have the ability to manage the new gTLD application process. In fact, adding numerous TLDs to the Root System may actually produce the unwanted and unintended consequence of creating instability and insecurity in the Internet infrastructure. Our comments above highlight the areas of greatest distress. We look forward to working with you, the ICANN Board of Directors and the ICANN staff in strengthening the DNS, and if found to be necessary, helping to explore ways to increase competition without creating the above noted negative externalities.

Given the above issues, we suggest that before ICANN proceeds with the new gTLD Program and Process, it should follow these recommendations:

---

[5] See http://www.icann.org/en/committees/tff/final-report-draft-30oct99.htm.

- Undertake the full economic study of the domain name marketplace mandated by the ICANN Board in 2007, as well as an extensive evaluation of whether new gTLDs are needed in the first place given the record of existing new gTLDs;
- Establish criteria for success of new gTLDs in the proposed first round – including Internationalized Domain Name TLDs – before moving forward;
- Modify the roll-out of the new gTLD program to only sponsored gTLDs and a limited number of IDN TLDs, once the study has been completed and criteria established; and
- Limit further roll-out until sufficient safeguards are in place to protect Internet users, businesses, and brand-owners alike from any existing and expected acts of cyber-fraud.

We respectfully request that the launch of the new gTLD program be delayed until these issues and recommendations can be adequately addressed.

Sincerely,

3M
AeA (Formerly the American Electronics Association)
Aerospace Industries Association
American Advertising Federation
Applied Materials, Inc.
CA, Inc.
Corning Incorporated
Dow Corning
Eaton Corporation
Gates Corporation
Illinois Tool Works Inc.
Information Technology Association of America
ITT Corporation
Intellectual Property Owners Association
Karsten Manufacturing Corp. & PING
MarkMonitor
Microsoft
National Association of Manufacturers
National Marine Manufacturers Association
NetChoice
The French Oil Mill Machinery Company
Tooling and Manufacturing Association
Uniweld Products, Inc.
U.S. Chamber of Commerce
Verizon
Yahoo! Inc.