
*Creating an online trust community, promoting business practices and technologies to enhance consumer trust and the vitality of interactive marketing, ecommerce and online financial services*

# Comments to ICANN on the New gTLD Program

Authored by

Craig Spiezle
Executive Director, OTA

Rod Rasmussen
President & CTO, Internet Identity
Member, OTA Steering Committee

November 30, 2009

---

**Background**
As an independent non-profit, OTA is a global organization addressing the end-to-end online trust issues and challenges faced by consumers, merchants and online financial services companies. OTA advances self-regulation and best practices through the Online Trust community. OTA represents a wide range of constituencies from leading interactive marketers, advertisers, and technology and solution providers to privacy advocates, academics, and merchant card processors. This autonomy helps to advance balanced recommendations and policies that are in the best interest of the consumer, while being practical and cost effective for businesses.

This document outlines some of OTA members' concerns and suggested remedies with the launch of new gTLDs by ICANN. OTA welcomes the opportunity to work with ICANN and other stakeholders to address these and other mounting concerns to help ensure a successful implementation of new gTLDs and other ICANN initiatives.

As the Internet has developed, the value proposition to consumers and business has grown exponentially. At the same time it has unfortunately attracted online crime and deceptive business practices, which are eroding online trust. Consumer anxiety continues to grow on multiple fronts: increases in identity theft, forged email and questionable data sharing practices combine together to collectively impact the promise of the Internet.

Based on a recent study from the National Cyber Security Alliance, 63% of respondents reported that they did not complete a Web site purchase because of security concerns, with the majority (62%) stating uncertainly of the web site as being a top concern.[1] Other research from OTA and member companies indicate over 80% of email sent daily is spam of which 30% upwards is malicious in nature.

The advent of gTLDs along with international character sets, introduces a wide range of concerns and potential implications, which may likely further diminish consumer trust and confidence if safeguards and ongoing monitoring are not established. Look-alike domains, drop catching, domain tasting, domain hijacking, and various deceptive practices have eroded consumer trust in domain names as a reliable Internet navigation method. While some of these issues have been addressed by ICANN actions and policies, we want to help to ensure that a major expansion in the available gTLDs also addresses trust and confidence issues that could otherwise compromise the long-term vitality of the Internet.

The following comments are in response to ICANN's New gTLD Program Explanatory Memorandum regarding Mitigating Malicious Conduct and the general issues surrounding the expansion of the gTLD universe.

[1] http://staysafeonline.mediaroom.com/index.php?s=43&item=54

## Vetted Registry operators

Ensuring that criminal organizations and deceptive businesses do not control or have direct access to registry operations is perhaps the most critical issue facing the introduction of a gTLD. Criminals have continually demonstrated the ability to inflict damage through fraudulent "reseller" fronts they have created for registering domain names. It is imperative that we prevent them from running an entire registry, or even placing people within a registry that would allow them unfettered access to create new, theoretically "bullet-proof" domains at will.

A correlation would be to a Certificate Authority being compromised and issuing bogus Extended Validation SSL certificates. The CA/Browser Forum has created safeguards including organizational vetting, auditing requirements, and a remediation process to revoke certificates improperly issued.[2]

We would like to see the proposal strengthened in two areas to address post-application operations. We are concerned that an abusive organization could be a "front" company with "clean" ownership to obtain rights to a registry. After creating this registry, the criminal organization could then take control after the vetting process had finished. Such organizations could acquire a registry via outright purchase without any review.

Short of running a registry, a criminal organization may also attempt to infiltrate one. This is common in many other industries, and we should not think that domain registries, especially in rapidly growing markets, would be immune from this tactic.

We request that the proposed background checks be performed beyond the application period, at a minimum at any point there is a registry ownership change and at contract renewal. Additional checks could be done at random intervals or in response to criminal complaints against a particular registry. Registries should be contractually bound to comply with such requests in order for these rules to have any real enforcement power.

Further, registry operators should be required to perform background checks on all key employees. This could be accomplished in many ways, including a third party to complete a "credit type check" on them. Results of those checks should be kept on-file, and updated on a regular basis. They should also be auditable by ICANN compliance staff at any time, either via direct communication with the background checking firm, or a trusted third party.

## Requirement for thick Whois records

We strongly support the requirement of thick Whois records for all registries. Today's lack of consistency of access to whois information can be a significant challenge for law enforcement as well as consumers who desire added information. Experiences with thin registries vary widely, with some registrars that appear to either not have whois properly provisioned, or face repeated systems breakdowns. Keeping whois information in thick format for all new registries will assist in tracking down information on a miscreant's registration activities. It will provide the ability to readily contact registrants of sites that have been compromised to assist them in securing them. Consumers also benefit from being able to investigate who owns a particular domain for a website they are interacting or conducting commerce with.

[2] See CA/Browser Forum http://www.cabforum.org/forum.html

**Treatment of Domain Name "Resellers"**
Accountability and transparency is a significant issue impacting the online trust ecosystem, and specifics as to the responsibilities and liabilities of so-called "resellers" of domain registrations have yet to be adequately addressed. Without better identification of who is providing such services using standards in whois and domain registration contracts, it may be impossible to tell who is responsible for actually handling the domain registration process and who "knows" the registrant. Without definitive accountability as to how registrars must deal with problem resellers or non-responsive ones, it is easy for miscreants to set-up shop under an inattentive registrar. Even with registrars that suspend problem resellers, the ability some registrars offer today for "instant" reseller sign-ups without strict verification of identities allows for miscreants to circumvent many measures designed to keep bad actors from providing domain registration services to criminals. It is our strong belief that this area needs more attention as part of the new gTLD process and to consider a process not unlike that for obtaining EV SSL Certificates. [3]

**Privacy & Data Sharing**
Data sharing with affiliates and third parties should be changed to an opt-in process, with clear and concise policies provide to businesses and user at point of customer interaction. The mounting abuse to such practices is currently under review by both the EU and FTC. It is suggested ICANN adopt the applicable OTA Online Trust Principles to proactively stem this practice http://otalliance.org/resources/principles.html

---

**About The Online Trust Alliance (OTA) https://otalliance.org**

The mission of OTA is to create an online trust community, promoting business practices and technologies which enhance consumer trust and the vitality of interactive marketing, ecommerce and online financial services

Through its member companies and organization affiliates, OTA represents over one million businesses and 500 million users worldwide with regional chapters in Asia Pacific, Canada and Europe. OTA is a 501c6 IRS-approved non-profit, governed by a Board and Steering Committee including Bank of America, BoxSentry, Datran Media, Epsilon, Goodmail Systems, Iconix, Internet Identity, Intersections, IronPort (a division of Cisco Systems), LashBack, MarkMonitor, Message Systems, Microsoft Corporation, McAfee, Publishers Clearing House, Return Path, Secunia, Symantec Corporation and VeriSign Inc.

For updated versions of this document visit https://www.otalliance.org/resources/initiatives.html

[3] https://www.otalliance.org/resources/EVresources.htm