THE CHERTOFF GROUP

September 17, 2013

Board of Directors
Internet Corporation for Assigned Names and Numbers
12025 Waterfront Drive, Suite 300
Los Angeles, CA 90094-2536

Re: ICANN Proposal to Mitigate Name Collision Risks

This public letter is submitted in response to ICANN's request for comment on the proposed efforts to mitigate potential impacts resulting from name collisions as new gTLDs are delegated, as described in the "New gTLD Collision Risk Mitigation Proposal" (August 5, 2013).

After studying certain risks associated with the proposed new gTLD program, The Chertoff Group is writing in support of calls for closer examination of stakeholder concerns expressed in this forum (see, for example, public letters submitted by VeriSign Inc., General Electric Company, and the Internet Service Providers and Connectivity Providers constituency to the ICANN forum regarding the "Proposal to Mitigate Name Collision Risks"). Specifically, before ICANN proceeds with the delegation of new gTLDs, we believe it is prudent to conduct additional analysis on the security and liability risks associated with these new gTLDs, particularly with regard to Critical Infrastructure and Key Resources (CIKR).

The Chertoff Group, a global security advisory firm, was retained by VeriSign, Inc. to independently assess the risk that the new gTLD program presents to CIKR. To accomplish that task, we conducted an informal outreach effort to CIKR operators, including knowledgeable individuals in the energy, information technology, and defense industrial base sectors, along with CIKR security experts, in order to develop a baseline understanding of what concerns, if any, independent operators and security experts have about risks stemming from the new gTLD program. By conducting an analysis of the existing literature on potential security and stability concerns posed by the new gTLD program, combined with outreach to operators in a subset of CIKR and experts on CIKR security, TCG was able to develop an understanding of how the new gTLD program might affect a range of key networks and thereby draw conclusions about the broad impact of the new gTLD program on CIKR.

Ultimately, our outreach indicated a systematic lack of widespread awareness and understanding of how ICANN's proposed expansion of new gTLDs—and resulting mitigation measures proposed by the Interisle Consulting Group, Certificate Authority/Browser Forum and other stakeholders—will impact the Domain Name System (DNS) and operators dependent on the operability of that ecosystem for critical infrastructure functions. Security mitigation plans were nascent and based on incomplete information, though most operators believed that, in the end, the security problems were capable of mitigation. But mitigation requires awareness. As a result, we believe that ICANN should undertake a broader awareness campaign to educate critical infrastructure operators on the identified risks and mitigation strategies related to the new gTLD program.

Based on our expertise and experience in the field, we are comfortable offering the observation that for domestic American activities the ideal method for disseminating information about the gTLD name collision concerns would be through the existing CIKR Information Sharing and Analysis Centers (ISACs) established for the sector-specific coordination and sharing of security-related information. This, indeed, would appear to be a function squarely within the operating remit of these organizations. We are aware of a limited number of private parties providing information to selected ISACs through in-person meetings and on-line alerts, but have yet to identify a systematic, coordinated education campaign. In light of this, we would urge engagement with the Department of Homeland Security to foster an awareness campaign as an effective means of implementing our recommendation domestically. It goes without saying, however, that any awareness program will also need to be implemented in non-American contexts, requiring different methodologies.

Notably, the core finding of our outreach study has already been stated by ICANN's own Security and Stability Advisory Committee (SSAC) in 2010. In SAC 045 "Invalid Top Level Domain Queries at the Root Level of the Domain Name System," the SSAC presents the following recommendation (emphases added in bold).

> *Recommendation (1): The SSAC recommends that* ***ICANN promote a general awareness*** *of the potential problems that may occur when a query for a TLD string that has historically resulted in a negative response begins to resolve to a new TLD. Specifically, ICANN should:*
>
> - *Study invalid TLD query data at the root level of the DNS and contact hardware and software vendors to fix any programming errors that might have resulted in those invalid TLD queries. The SSAC is currently exploring one such problem as a case study, and the vendor is reviewing its software. Future efforts to contact hardware or software vendors, however, are outside SSAC's remit. ICANN should consider what if any organization is better suited to continue this activity.*
> - *Contact organizations that are associated with strings that are frequently queried at the root. Forewarn organizations who send many invalid queries for TLDs that are about to become valid, so they may mitigate or eliminate such queries before they induce referrals rather than NXDOMAIN responses from root servers.*
> - *Educate users so that, eventually, private networks and individual hosts do not attempt to resolve local names via the root system of the public DNS.*

The issue of awareness and education was so fundamental to mitigating the concerns surrounding the new gTLD program that the SSAC made it the first recommendation in its report on name collisions in the DNS. Yet, we were surprised to discover a lack of educated awareness and mitigation strategies across certain CIKR operators.

In conjunction with this effort, members of The Chertoff Group also reviewed Verisign's study—published to the ICANN name collision forum on September 15th— of the queries being directed towards the proposed new gTLD .cba, which Interisle Consulting Group classified as "uncalculated risk." This study methodically characterizes a number of security risks associated with the .cba gTLD and, in our view, begins to bring to light a number of liability concerns that have received limited scrutiny in public discussion on gTLD delegation. Looking to the example of .cba presented in Verisign's analysis, it is very challenging to estimate the cost or resources necessary to mitigate this potential vulnerability. For example, if Japanese high-rises using .cba namespaces in operating infrastructure were targeted by a malicious actor exploiting vulnerabilities resulting from the ambiguity in naming, the result could be disabling or disrupting critical functions in these residential buildings. The applicant for the .cba gTLD would be liable for any subsequent damages, pursuant to ICANN's recently announced risk mitigation plan. Such liability could prove devastating to smaller organizations commissioning new gTLDs, ultimately undermining ICANN's objective to enhance consumer trust and business opportunity in the market place.

Though we are cognizant of the commercial pressures that underlie the need for prompt initiation of the gTLD expansion program, The Chertoff Group is of the view that existing awareness of potential security risks in the CIKR community is incomplete and inadequate. Nor does it appear that applicants for new gTLD strings fully understand associated liability risks. We believe that additional study and analysis of both security and liability questions would be beneficial to all stakeholders in the new gTLD program.

Sincerely,

Michael Chertoff
Chairman
Chertoff Group, LLC