gTLD String: Tickets
Applicant Entity Name: Shubert Internet, Inc.
Application ID#: 1-1973-48269

SPECIFICATION 11
PUBLIC INTEREST COMMITMENTS

We are committed to responsible self-governance and look forward to finalizing the PIC program into a safeguard that encourages consumer choice and competition and assures the security and stability of the Internet. In furtherance of those goals, we offer the following commitments:

1. Registry Operator will use only ICANN accredited registrars that are party to the Registrar Accreditation Agreement approved by the ICANN Board of Directors on [date to be determined at time of contracting], 2013(or any subsequent form of Registrar Accreditation Agreement approved by the ICANN Board of Directors) in registering domain names. A list of such registrars shall be maintained by ICANN on ICANN's website.

2. [Intentionally left blank]

3. Consistent with the representations made in our application and with reference to the Government Advisory Committee Toronto Communiqué (October 17, 2012); the United States Government (USG) Input to Early Warning Processes for New Generic Top-Level Domain Names (gTLDs) Via the Governmental Advisory Committee; and the letter from Lawrence Strickling of the U.S. Department of Commerce to Dr. Stephen Crocker, Chair of the Board of Directors of ICANN, dated February 26, 2013, we make the following commitments:

We will implement and operate a robust abuse mitigation process to minimize abusive registrations that have a negative impact on Internet users and rights holders. We commit to establish and promulgate an Acceptable Use Policy (AUP) for registrants, which will feature enforceable processes designed to ensure that registered domain names will be used only for legitimate activities. Our AUP will include but is not limited to the following commitments we agree to be bound by within the confines of applicable laws:

- To publish and make readily available to the public policies and procedures that cover domain name acceptable use, naming standards, and which define malicious or abusive behavior. Abusive behavior includes, but is not limited to, using domain names for spam, phishing, pharming, and illegal activity, as well as cyber squatting or other behavior that infringes the rights of others;

- To make these policies and procedures binding upon registrants by requiring registrars to get registrant agreement to our AUP as a condition of registration during the sign-up process;

- To provide an easily accessible flagging process that allows members of the public, law enforcement, and other government entities to quickly and easily call attention to possible cases of non-compliance with these policies or to report abuse;

- To provide a single point of contact, available to law enforcement and other authorized government entities, responsible for addressing reports of abuse, non-compliance and other matters requiring expedited attention;

- To constructively work with law enforcement to address reported cases of abuse;

- To timely review, resolve, and respond to reported cases of abuse, including implementation of procedures that allow us, within the confines of applicable laws and in cases where domain registrations are determined to have been used abusively, to:

    - Suspend or delete abusive domain names;
    - Block registrants of abusive domain names from further registrations; and/or

    - Suspend or delete all names associated with a registrant.

- To prevent registration of exact matches of geographic names at the second level as defined by the Applicant Guidebook of January 12, 2012, except by authorized representatives of the governmental authority of the territory in question;

- To prevent registration of exact matches of IGO names at the second level, according to the list to be provided by the GAC as per the GAC Toronto Communiqué of 17 October 2012, except by authorized representatives of the IGO in question;

- To institute a 60-day Trademark Sunrise using the Trademark Clearinghouse process;

- To develop a dispute-resolution procedure that supplements ICANN-mandated processes, including access to alternative resolution processes; and

- To implement security policies and procedures commensurate with the security profile of the TLD.