COALITION FOR ONLINE ACCOUNTABILITY

WWW.ONLINEACCOUNTABILITY.NET

C/O MITCHELL SILBERBERG & KNUPP LLP ● 1818 N STREET N.W., 8TH FLOOR ● WASHINGTON, D.C. 20036-2406
TEL: (202) 355-7906 ● FAX: (202) 355-7899 ● E-MAIL: INFO@ONLINEACCOUNTABILITY.NET

Memorandum

To: Dr. Stephen D. Crocker, ICANN Board Chair
Rod Beckstrom, ICANN President and CEO

From: Steve Metalitz, Counsel to COA

Re: Proposed Enhanced Safeguards for New gTLDs Targeting Creative Sectors

Date: March 6, 2012

I am pleased to submit to you proposed criteria for use by ICANN evaluators in applying ICANN evaluation criteria 28 (Abuse Prevention and Mitigation) and 30 (Security Policy) to new gTLD applications that target industry sectors dependent on copyright protection.

These criteria are endorsed not only by the Coalition for Online Accountability (see below for names of participating organizations) but also by major international organizations representing the creative industries, including the International Federation of the Phonographic Industry (IFPI); the International Video Federation (IVF); and the International Federation of Film Producers Associations (FIAPF). The criteria are also supported by the leading organizations for independent music and film, including the American Association for Independent Music (A2IM) and the Independent Film and Television Alliance (IFTA).

We strongly believe that the application of these guidelines in the evaluation process will promote the use of new gTLDs in this sector for legitimate and law-abiding purposes, while reducing the real risk that these registries will become havens for piracy or other online abuse. We urge ICANN to provide these criteria to the contractors who will be carrying out the evaluation of new gTLD applications, as an example of "security measures [that] are appropriate for the applied-for gTLD string." Given the continuing vulnerability of creative industries to services built on copyright theft online, we believe that new gTLDs targeted to copyright industry sectors clearly fit the "exceptional potential to cause harm to consumers " criterion that the Applicant Guidebook uses to describe applications for which enhanced safeguards are appropriate.

We will be encouraging national governments to apply these criteria in their review of new gTLD applications in the Early Warning phase of the new gTLD process. We also plan to use them in preparing public comments on relevant applications, and will, of course, be sharing them with potential applicants for new gTLDs targeting our sector.

Please let me know if you have any questions or would like further information about the enhanced safeguards document attached.

New gTLDs Targeting Creative Sectors: Enhanced Safeguards

ICANN's recent launch of a program to accredit hundreds or thousands of new generic Top Level Domains (gTLDs) has the potential to create new opportunities and to better integrate the creative sectors with the digital economy But the launch is also fraught with serious risks to those engaged in creating, producing and disseminating creative works – music, movies, videogames, entertainment software, and more. All these sectors have historically been vulnerable to online theft, infringement and other fraud, and continue to experience unacceptably high levels of such abuse. **If new gTLDs targeted to these sectors – e.g., .music, .movies, .games – are launched without adequate safeguards, they could become havens for continued and increased criminal and illegal activity.** That would be disastrous for the creative sectors worldwide, and thus for jobs, economic growth and competitiveness in many countries.

In evaluating applications for such content-focused gTLDs, ICANN must require registry operators (and the registrars with whom they contract) to implement enhanced safeguards to reduce these serious risks, while maximizing the potential benefits of such new domains. **Governments should use similar criteria in the exercise of their capability to issue Early Warnings**, under the ICANN-approved process, with regard to new gTLD applications that are problematic from a public policy or security perspective.

The following criteria comprise a high-level statement of **the minimum safeguards that should be demanded of new gTLDs targeted to the creative sectors.** Their aim is not hinder legitimate business models in these new gTLDs, but to provide fair and efficient mechanisms for preventing abuses and dealing with them if they do arise. ICANN has already received proposed enhanced safeguards formulated by representatives of the financial services industry, and acknowledged them in the January 2012 Applicant Guidebook as an "illustrative example" of an independent security standard that should be considered in the new gTLD evaluation process. These guidelines provide another such example, with some overlap in safeguards, and could also help provide a template, with appropriate modifications, for other gTLDs targeted to groups or industry sectors that are especially vulnerable to online fraud or abuse, including counterfeiting.

1. **Authenticated, Verified, Publicly Accessible Whois Data:** it must be known who is registering at the second level in these domains. At the time of registration, registrars should be required to verify that the person or entity claiming to be the registrant exists, the data is not fraudulent, and the person or entity can be located and contacted. Registrations from serial violators of registry standards should also be screened out. If proxy registrations are not prohibited, then the registry operator must have real-time access to verified registrant contact data for audit purposes and for prompt resolution of complaints (see below).

2. **Enforceable Certification by Registrant** that the domain name will be used only for licensed, legitimate activities, and not to facilitate piracy or counterfeiting. This requirement should be incorporated in a registry Acceptable Use Policy that is publicly disclosed and with which all registrants must certify their compliance before registration and periodically thereafter.

3. **Proactive Auditing by Registry/Registrar** that certification is being respected. Appropriate remediation steps should follow when violations are detected.

4. **Prompt, Accessible Mechanism for Right Holder Complaints** that certification is being violated or that piracy, counterfeiting or other abuses are being enabled. Complaints should trigger an expeditious investigation, with prompt notice to registrants, a reasonable opportunity for them to respond, and swift corrective action when violations are found.

5. **Predictable Consequences for registrants who violate certification,** allow infringing activities, falsify registrant contact data, etc. Potential consequences may include cancellation of the

registered domain where the abuse occurs; possible cancellation of other domains registered by same or affiliated parties; and bar on future registrations by same or affiliated registrant, in the case of serial offenders.

6. **Seats at the table for right holders** as registry policies reflecting these safeguards are developed, implemented, and enforced.

7. **Demonstrable evidence that the registry has the capability and commitment, and will devote the needed resources**, to implement the preceding safeguards effectively.