CADNA
The Coalition Against Domain Name Abuse

February 15, 2008

Suzanne R. Sene
Office of International Affairs
National Telecommunications and Information Administration
1401 Constitution Ave., N.W., Room 4701
Washington, D.C. 20230

Re: Midterm Review of the Joint Project Agreement (Docket No. 071023616-7617-01)

Dear Ms. Sene:

Please accept these comments from CADNA, the Coalition Against Domain Name Abuse, on the Mid-Term Review of the Joint Project Agreement between ICANN and the US Department of Commerce

NTIA has instituted a public review of ICANN's progress towards becoming "a more stable organization with greater transparency and accountability in its procedures and decision making" that is essential for a fair and accurate assessment of whether ICANN is ready to complete the transition of Internet DNS management to the private sector.

CADNA welcomes the opportunity to comment on ICANN's comments and efforts to establish that it is prepared to function as a fully independent body without public oversight.

I. JPA Responsibility Milestones

CADNA believes that ICANN has not made sufficient progress on a number of key Responsibilities outlined in the Joint Project Agreement (JPA) to demonstrate that it is ready to be released from the oversight role of the U.S. Department of Commerce.

For example, ICANN has not maintained and built "processes to ensure that competition, consumer interests, and Internet DNS stability and security issues are identified and considered in TLD management decisions, including the consideration and implementation of new TLDs." NTIA Request for Comments No. 5 at http://www.ntia.doc.gov/ntiahome/frnotices/2007/ICANN_JPA_110207.html.

- ICANN has failed to take effective steps to curb the abuse of the Add/Drop Grace Period (AGP) by domain name monetizers and collaborating registrars. On the contrary, it has endorsed an ineffectual proposal for a 20-cent restocking fee for each domain returned during the AGP that will line ICANN's pockets but do little to deter cybersquatters.

- ICANN has openly tolerated registrar practices that run directly counter to competition and consumer interests, such as Network Solutions' five-day "reservation" of every available domain name that the public queries on its Whois database.

- While ICANN has indicated its intention to launch 900 new TLDs in the next three years, it is considering GNSO recommendations that would eliminate normative evaluation of both the need for new TLDs and of the suitability of the registry applicants.

ICANN has also failed to "implement measures to maintain timely, unrestricted and public access to accurate and complete WHOIS information, including registrant, technical, billing and administrative contact information." NTIA Request for Comments No. 5 at http://www.ntia.doc.gov/ntiahome/frnotices/2007/ICANN_JPA_110207.html.

- Despite rampant false Whois data and unhelpful registrars that act as gatekeepers between deceptive registrants, on the one hand, and law enforcement and trademark owners, on the other hand, ICANN has done little to eliminate practices that inhibit unrestricted public access to accurate and complete Whois information, such as private registration services. By concealing a registrant's identity, such practices frustrate the efforts of law enforcement and brand owners to protect the public from fraud and deception.

- In fact, ICANN is headed in the opposite direction: it recently endorsed a proposal to *further restrict* public access to Whois information by instituting a policy that would replace a domain name registrant's postal address, city, postal code and administrative and technical contacts with an "Operational Point of Contact" (OPOC). Far from increasing access to accurate Whois information, the OPOC policy would erect yet another barrier to unrestricted access to such information.

Nor can it be said that ICANN has "devoted adequate resources to contract enforcement." NTIA Request for Comments No. 10 at http://www.ntia.doc.gov/ntiahome/frnotices/2007/ICANN_JPA_110207.html.

- Despite ICANN's Registrar Accreditation Agreement (RAA), which requires accurate information upon registration, registrars continue to enter obviously false data during the application process.

- ICANN has failed to develop an effective mechanism to ensure that registrars abide by the terms of the RAA. Since ICANN's sole penalty for violation of the RAA is to revoke a registrar's accreditation, it has been understandably reluctant to take that drastic step in

all but a single case. ICANN cannot justify its failure to implement any enforcement mechanisms against registrars that are known to be violating the RAA in many significant and material ways.

Further, ICANN has failed to improve significantly on "accountability mechanisms to be responsive to global Internet stakeholders… including continuing to improve openness and accessibility for enhanced participation in ICANN's bottom-up participatory policy development process." NTIA Request for Comments No. 3 at http://www.ntia.doc.gov/ntiahome/frnotices/2007/ICANN_JPA_110207.html.

- Many of ICANN's problems stem from the overrepresentation of the interests of a single constituency in its governance, namely registrars and registries, at the expense of all other stakeholders, including consumers, the IP community and law enforcement. Time and time again, ICANN has shown that it is willing to sacrifice the interests of the larger Internet community in favor of the narrow interests of a single group of stakeholders. Until this imbalance is corrected, CADNA believes that the NTIA cannot leave ICANN without any public oversight.

II. A Question of National Interest

Beyond the desire to make the Internet a safer place for the entire international community at large, the prospect of ICANN independence has implications specifically for the national security interests of the United States. An increasing amount of industrial espionage is conducted via the Internet. Therefore, the United States has a vested interest in maintaining oversight over the Internet's governing body to protect critical government systems, financial systems, and public infrastructure from Internet-based attacks. In order to pursue actors who use the Internet to exploit the public and commit "virtual crimes," law enforcement must be able to access critical information controlled by ICANN.

III. Conclusion

ICANN must develop a structure that will fairly represent and protect *all* Internet stakeholders. Until then, NTIA must retain its oversight over ICANN.

Sincerely,

Joshua S. Bourne
President
The Coalition Against Domain Name Abuse