June 8, 2009

Fiona M. Alexander, Associate Administrator
Office of International Affairs, National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, N.W.
Room 4701
Washington, DC 20230

Dear Administrator Alexander:

Thank you for the opportunity to comment on the state of the Joint Project Agreement (JPA) between the NTIA and ICANN, and to provide our feedback and views on the effectiveness of ICANN in meeting its obligations to the broad internet community, its direct stakeholders, and its obligations under the JPA.

Our commentary will focus on several areas:

1. ICANN's role and success in promoting the safety, security, and stability of the DNS;
2. Overall governance and accountability issues of ICANN;
3. Areas of governance that need more focus.

We support the ongoing oversight of ICANN by the NTIA via the JPA to ensure that certain concerns are addressed with regard to the security of Internet users.

Regarding the questions presented in Item 1 and Item 5 within the mid-term review of the JPA:

> Item 1. The DNS White Paper articulated four principles (stability; competition; private, bottom-up coordination; and representation) necessary for guiding the transition to private sector management of the DNS. Are these still the appropriate principles? If so, have these core principles been effectively integrated into ICANN's existing processes and structures?
>
> Item 5. The current JPA called for NTIA to conduct a mid-term review. That review revealed that ICANN needed to take further steps to increase institutional confidence related to long-term stability, accountability, responsiveness, continued private sector leadership, stakeholder participation, increased contract compliance, and enhanced competition. What steps has ICANN taken to address the concerns expressed in the mid-term review process? Have these steps been successful? If not, what more could be done to meet the needs of the community served in these areas?

ICANN has shown the ability to address most of core principles set out in Item 1 during the term of the existing JPA. However, ICANN has been slow to adapt to the recent increase in sophistication and proliferation of Internet based crime. As such, we believe a new core-principle should be added -- not to address the security of the DNS infrastructure itself, but rather to address the security of those who make use of the DNS infrastructure -- namely general Internet users. Of course, this is not to suggest that ICANN can unilaterally protect Internet users from all harm, or that other parties are without responsibility in this too. However, ICANN must have a role in doing what it reasonably can to protect Internet users from e-crime.

We welcome the recent announcements related to the security and stability of the DNS system and the proposal to rapidly implement DNSSEC signing of the root zone. Consistent with our

feedback during the comment period on DNSSEC operational models, DNSSEC should be rolled out expeditiously and not delayed while an overall governance model is created.

Protecting the security of Internet users is paramount in ensuring confidence in ecommerce, buying and selling on the Internet, and ICANNs public perception. In the past two years, attacks have become more sophisticated (see: Initial Report on Fast Flux Hosting)[1] and yet the remedies and process to address these attacks within ICANN and DNS infrastructure has not. While a report on Fast Flux Hosting is useful, more of these studies must be conducted to address other attacks that ICANN or ICANN members can play a role in preventing and addressing. ICANN must take immediate steps within the scope of its role to promote the safety of Internet users.

Additionally, ICANN must become more active in areas of internet unique identifier governance than it has in the past – namely the governance of IP addresses, and the WHOIS data related to them. Modern attacks on the internet do not always rely on domain names and the registry/registrar community to work. Some attacks are simply using IP addresses as identifiers, and without broader coordination and action from ICANN related to WHOIS correctness for IP address blocks these attacks will persist and worsen.

In addition to IP WHOIS correctness, we believe that the scope of the arrangements between ICANN and the RIRs should include contractual provisions that explicitly address the same areas that Registry agreements include – specifically those sections dealing with appropriate use and abuse. Whereas registries and registrars currently act to enforce abuse policies against domain name owners, no such enforcement mechanisms exist for the RIRs and ISPs with delegated address blocks. While such agreements may be outside ICANN's remit, encouraging such provisions in RIR operating agreements and with the NRO should be one of ICANN's roles as a governing body for IP address block allocation.

Finally, there is the thorny subject of oversight and governance of ICANN itself. At a fundamental level, there only seem to be three major alternatives: some form of continued lightweight oversight of ICANN by NTIA; transfer of oversight to an international organization, presumably the ITU; or a self-governing model where ICANN is completely self-managed. It is fair to say that none of these models are perfect and there are practical objections to all of them. In this regard, we believe that the decision should be based on choosing the "least worst" option.

In our assessment of these options, we believe that the ITU is a credible body for oversight of existing telecommunications infrastructure where such infrastructure and standards are well understood and stable. However, it has no meaningful track record of oversight of rapidly evolving areas such as the Internet, and we believe that the well-known politics that occurs in the ITU prevent it from making rapid and effective decisions. These characteristics render it almost wholly unsuitable for any practical oversight over ICANN.

ICANN has many admirable qualities as an Internet governance authority. While it has been slow to act on some issues, and has been constrained by the contract-driven nature of its relationships with registrars and registries, it is nonetheless clearly trying to be even-handed and proactive. Unfortunately, it also suffers from some oddities in its own governance. In particular, it has historically been dominated by those with self-evident commercial interests, and its policies for long periods of time have tended to reflect those quite narrow interests. Without some level of independent oversight, we believe it is credible to imagine scenarios wherein ICANN would effectively be muzzled by these parties from taking actions that might be needed to protect the general availability, safety and security of the Internet. The current proposals for ICANN to be

fully self-governed do not seem to contemplate the possibility of such an eventuality, and seem to us therefore, unwise.

There are many well-documented concerns about oversight of ICANN by NTIA, and the possibility of abuse by the US government, that this relationship might enable. In practice, there is not a single shred of evidence of such abuse ever having occurred. We do not therefore support terminating the JPA, and allowing ICANN to be fully self-governing. Nor would we support a short extension of the JPA, as we believe that there are no credible alternatives other than the two described above. Instead, we feel that the JPA should be renewed – albeit with changes, as described herein – for a lengthy period, perhaps five or ten years.

Recommendations
==========

In order to maintain security for Internet users, those who attack Internet users must be identified and swift action to shutdown their attacks must be taken. Often, domain information and WHOIS data is inaccurate or faked in order to obfuscate the true source of these attacks. ICANN has taken steps to improve the data accuracy within the WHOIS database, however more improvements are necessary. The Whois Data Problem Reporting System (WDPRS) is a good first step, but too many people are unaware of its existence or lack confidence in the WDPRS itself.

As such, we would like to provide the following recommendations:

1. Add "security of Internet users" (within the scope of ICANN, DNS, and Registrars) to one of the core principles within the JPA and support this core principle with specific actions ICANN and Registries can take to improve and enhance the security of Internet users. The "Initial Report on Fast Flux Hosting" is a good first step -- expand that to include other significant risks that are inherent within the DNS system.

2. Regarding the Whois Data Problem Reporting System: To obtain a higher level of inaccurate WHOIS data reports, consider including the URL pointing to the WDPRS within the data returned during a WHOIS lookup. Too many abuse departments are trained to email the "Abuse Contact" listed within WHOIS. Sometimes those contacts are bogus, fake, or participating in the abuse themselves. ICANN must ensure both the accuracy of the WHOIS data, so reports go to someone who can review and take action, as well as provide some type of statistics or reporting on what registries are receiving the majority of abuse reports and whether they are being appropriately acted upon or ignored. By adding the WDPRS URL to the data returned during a WHOIS query, more reports will be provided by those who see inaccurate data, and the accuracy level of the WHOIS data will improve.

3. Increase the scope of ICANN's role of coordinating policy with the RIRs to provide better policing of WHOIS correctness related to IP information. Because of a current lack of accountability by the RIRs, and proper policies and processes in this area, the accuracy of WHOIS for IP blocks is even more susceptible to abuse than that for domains.

4. Organized Electronic Crime entities are creating their own registrars or are enabled by existing registrars who are turning a blind eye to criminal actions. The "Proposed Registrar Disqualification Procedure" policy [2] currently under ICANN review will help address this problem assuming it is implemented properly. We ask that ICANN consider using the existing framework of the "Uniform Domain-Name Dispute-

Resolution Policy" (UDRP) process. There should be a mechanism by which registrars who are egregious in their hostile activity can have a dispute filed against them as exists for domain names within the UDRP. Allowing other entities to file a dispute against only the most egregious registrars would result in improved monitoring and deterrence of hostile registrar activity.

On the question of accountability of ICANN, we have general concerns related to the structure and nature of the ICANN board, the stakeholders concept, and the limitations of ICANNs scope to not include the safety and security aspects of its governance as they apply to the general internet user. The gTLD process has shown that the existing process, the stakeholder model, and ICANN's reluctance to follow through on certain requirements of its stakeholders, such as a reasonable economic study of the gTLD process, isn't working as well as it could.

5. The JPA should be renewed, with the recommendations described above, for a lengthy period – at least five years, and possibly ten. While this model suffers from theoretical concerns about political independence, it seems to us to be the most pragmatic option and by far the least risky in practice. Given that such changes have the potential to negatively impact the stability, safety and security of the Internet ecosystem, we do not believe that the risk/reward ratio justifies any serious oversight change.

Finally, in closing we would again like to thank the NTIA for the opportunity in commenting on this vitally important topic. The future of ecommerce could very easily rest upon this decision, and we are pleased to be able to contribute, in any small way, to the debate about how this can be assured. I would also like to publicly note the vital contribution of two of my team members – Andy Steingruebl, and Jon Orbeton – in the formulation of PayPal's thinking on this question.

Sincerely,
Michael Barrett
Chief Information Security Officer, and VP Information Risk Management, PayPal

[1] Initial Report on Fast Flux Hosting: http://gnso.icann.org/issues/fast-flux-hosting/fast-flux-initial-report-26jan09.pdf
[2] Proposed Registrar Disqualification Procedure: http://www.icann.org/en/registrars/draft-disqualification-procedure-27feb09-en.pdf