IPC Comments:
New gTLD Program Explanatory Memoranda
Mitigating Malicious Conduct &
A Model for a High Security Zone Verification Program

November 22, 2009

The IPC strongly supports community efforts to address malicious conduct in the Internet's domain name system (DNS). Current levels of malicious abuse in the DNS remain at unacceptably high levels for the Internet user community. Any increase in the number of gTLDs threatens to exacerbate these risks. As cited in the most recent Anti Phishing Working Group report on phishing activity: "…malicious domain name registrations do remain a damaging part of the current phishing problem, since they are used by the most prolific phishing gangs, which use them to harbor multiple phishing attacks…the first half of 2009 saw a rise in the number of hijacked brands to a record 310 in March, up more than 5 per cent from the record of 294 reached in May, 2008 and January, 2009….Phishers continue to expand the number and kind of brands they attack, and to employ fast-flux schemes to relocate phishing servers from one compromised host to another…As we have observed in the past, the domain name itself usually does not matter to phishers, and a hacked domain name of any meaning, in any TLD, will usually do…" *APWG Global Phishing Survey: Trends and Domain Name Use 1H2009*

The IPC has considered the proposals contained in the Explanatory Memorandum on Litigating Malicious Conduct (see http://www.icann.org/en/topics/new-gtlds/mitigating-malicious-conduct-04oct09-en.pdf) in the context of this reality, and has concluded that proposed procedures are inadequate. While the IPC applauds the recent efforts of ICANN staff and community members to develop measures to address malicious conduct issues in new gTLDs, the IPC believes that additional security measures must be developed and that existing mechanisms must be improved to protect consumers from further harm in the domain name space.

While ICANN has cited numerous sources as the genesis of the current staff proposals, the IPC believes that a more unified and comprehensive approach is warranted to address this monumentally large problem. The IPC recommends that ICANN continue on its efforts by forming a group of experts drawn from the GNSO and broader Internet community to develop proposals for addressing malicious conduct in new gTLDs. The group's outcomes should be subjected to an independent community review and separate public comment period on the ICANN website. Proper time and due consideration must be provided in order for the community to fully understand the implications that new procedures might have on Internet users and contracted parties.

The IPC welcomes the opportunity to provide comments on the issues raised in the Explanatory Memorandum. We offer the following overall recommendations:

Recommendation #1: all proposed mechanisms designed to mitigate malicious conduct should be considered required elements of the new gTLD program, not voluntary options. ICANN

might consider granting exceptions in rare cases to registry operators, but only when justified by exceptional circumstances. By imposing mandatory contractual provisions on registry operators, ICANN will ensure that anti-abuse proposals are not gamed and that loopholes in security provisions are closed to the maximum extent possible. Mandatory provisions will also ensure that ICANN does not evolve into a "certification agency" for the domain name security industry, but will remain committed to its proper role as the central technical coordinator of the Internet's unique identifiers.

Recommendation #2: a non-trademark related Rapid Domain Name Suspension Process should be developed to address malicious conduct in new gTLDs. The IPC believes that such a process is a key component in any set of procedures aimed at addressing malicious conduct in new gTLDs.

Recommendation #3: current procedures used to register gTLD domain names, and to deal with DNS-related abuse issues, must be improved, in order to ensure the integrity of domain names and registry data. Existing shortcomings in these procedures will carry over to new gTLDs where new registry operators will be less prepared to deal with malicious conduct and the resulting consumer harm.

IPC offers the following responses to the questions posed on page 5 of the Explanatory Memorandum under "Key Issues Identified":

A. How do we ensure that bad actors do not run Registries?

The Memorandum's solution to prevent bad actors from involvement in registries is to provide for vetting of all registry applicants. It is commendable that ICANN proposes to conduct background checks on new gTLD applicants, and that it has expanded the scope of potential disqualification of applicants, including in some areas advocated by IPC in its comments on the "excerpts" to DAG v.3. However, the mechanism proposed remains deficient in a number of ways.

As an initial matter, the vetting process only examines the officers, partners, directors, managers, or other affiliates or persons owning more than 15% of an applicant during the application process. Experience teaches that bad actors will frequently create shell companies and other legal vehicles to hide behind. ICANN ought to be given the flexibility to deny a "bad actor" applicant which it uncovers is an "alter ego", "related entity" or "funder" of the applicant. It should also be able to disqualify, not just on the basis of the past record of an entity owning 15% or more of the applicant, but also on the record of that entity's officers, directors, or controlling stockholders.

Another deficiency in the Memorandum is that it examines the registries only during the application process. While these are laudable steps, ICANN's must also police registries that

become bad actors, or that enter into business with bad actors, after they are approved. Meaningful enforcement mechanisms for injured parties must be in place to address registries that engage in behavior such as that outlined in subsections (a) though (f) of the proposed disqualification criteria on page 7 of the Explanatory Memorandum.

ICANN's track record in the registrar sphere does not yet provide sufficient assurance here. Although ICANN claims to follow up on all complaints concerning RAA violations, it does not have a well-publicized process to allow third-parties to submit complaints to ensure enforcement of registry agreements. Furthermore, there is no transparent or set process and remedies or sanctions for violations of the RAA. See e.g., http://www.icann.org/en/compliance/compliance-flowchart.htm.

ICANN needs to have the ability to audit registries, both to ferret out false statements with regard to disqualification that are made in the application process (the current version of the draft registry agreement does not authorize such audits), and to investigate whether a registry that was not disqualified at the time of application has become disqualified subsequently. Additionally, ICANN should consider conducting a similar or identical vetting process on applicants that have been delegated the right to operate a new gTLD on a periodic basis (e.g., every three years).

B. How do we ensure integrity and utility of registry information?

The Memorandum seeks to ensure security of the DNS by requiring DNSSEC deployment, prohibiting wild carding and encouraging removal of Orphan Glue records. As discussed herein, these standards must be backed up by sufficient enforcement mechanisms. Furthermore, ICANN's domain name registration process must be reformed (whether through the RAA or other contractual changes) to ensure the integrity of domain name registration data. Absent such domain name registration process reforms, other mechanisms designed to address malicious conduct in new gTLDs will fall short of reaching their goals, since the underlying process for registering domain names does not ensure the integrity of the registry data, and can be so easily manipulated by nefarious actors seeking to defraud consumers.

C. How do we ensure more focused efforts to combating identified abuse?

The Memorandum identifies four factors to combat abuse: requiring thick WHOIS records, centralizing of zone-file access, documenting registry and registrar level abuse contacts and policies, and making an Expedited Registry Security Request process available. IPC believes that a security-related rapid suspension process must be added to this list.

The endorsement of the IRT's Thick WHOIS requirement is a positive step, but again, there needs to be a transparent and set process for third-party complaints, an adjudicative process, and remedies or sanctions that deter or prevent malicious conduct. Although WHOIS records are currently required to contain truthful information, malicious actors virtually always

use false information and many WHOIS records still contain such false information. ICANN should place an emphasis on the accuracy of WHOIS information, which is currently not referenced in the Memorandum. It should also require, as part of the registry agreement, that new gTLD registries spell out their policies to require registrars (who collect Whois data in the first place) to ensure the accuracy of that data, to respond promptly and effectively to reports of false Whois data, and to swiftly cancel registrations that are based on false Whois data that is not promptly corrected.

Proxy/private domain name registration services, which are often used by malicious actors, also represent a problem, to the extent they are allowed in the new gTLDs. ICANN must develop a process to ensure that these services comply with the provisions of ICANN's contracts. These services often render the Thick WHOIS goals ineffective, and are likely to do the same in the new gTLDs unless the problem is anticipated. ICANN should require that the contact information behind such private registrations be accurate, and that the private registration services disclose the true identity of the registrant of a domain name when a rights holder or injured party can show that it has not received a response to sufficient allegations of harm or if certain allegations are implicated by the registrant's use of the domain name. ICANN oversight in this area is currently insufficient, and as a result, law enforcement and private parties face extensive difficulties in preventing both civil and criminal fraud on the Internet. New processes and guidelines must be developed to ensure that privacy/proxy services comply with their contractual obligations.

Finally, with respect to phishing scams and other criminal acts undertaken by registrants, meaningful enforcement must be swift, in the form of a rapid takedown requirement, a system similar to the proposed Uniform Rapid Suspension system dealing with cybersquatting. It should be noted that a "rapid takedown or suspension system" is recommended by the Memorandum but only with respect to orphan glue records being used for phishing. The requirement should be that all new gTLD registries put in place such a rapid take down system for addressing any criminal and fraudulent domain name use.

D. How do we provide an enhanced control framework for gTLDs with intrinsic potential for malicious conduct?

The IPC supports in principle the High Security Zones Verification Program, as set out in the second Explanatory Memorandum (see http://www.icann.org/en/topics/new-gtlds/high-security-zone-verification-04oct09-en.pdf) but believes that any proposed control framework must be mandatory on all new gTLDs to ensure that the benefits of the program extend across a potentially drastically expanded domain name space. The IPC believes that all new gTLDs contain an intrinsic potential for malicious conduct, and as such, require increased zone security provisions to mitigate the risks to Internet users and consumers. At a minimum, compliance with the program should be the norm for all applicants, leaving open the possibility that an applicant could be granted an exception if it can demonstrate that it has put comparable safeguards into place.

IPC appreciates the opportunity to comment on the Memorandum and looks forward to working with ICANN and with other interested parties toward improved safeguards against malicious behavior in the new gTLDs.