New Registry Service Proposal
.INFO Abusive Domain Use Policy

Proposed Service

***Name of the Proposed Service**:* .INFO Abusive Domain Use Policy

Technical Description of the Proposed Service*:*

Abusive uses of domain names, such as phishing, spamming, and distribution of malware, are a growing problem across the Internet. These behaviors are increasingly perpetrated by professional criminals who use technically and socially sophisticated means to victimize the public and misuse Internet resources.

This new policy, to be adopted pursuant to section 3.5.2 of the .INFO Registry Registrar Agreement, is designed to benefit registrants, registrars, and end-users of .INFO domain names across the Internet. It will more explicitly define illegal and abusive practices with respect to .INFO domain names, and will set expectations regarding the mitigation of these issues.

The proposed policy is as follows:

****

.INFO Abusive Domain Use Policy

The following policy ("Abusive Domain Use Policy") is announced pursuant to section 3.5.2 of the Registry-Registrar Agreement ("RRA") in effect between Afilias and each of its Registrars, and is effective upon thirty days' notice by Afilias to Registrars.

Registrars should not tolerate abusive use(s) related to .INFO domain names for which they act as sponsoring registrar. The nature of such abuses creates security and stability issues for the registry, registrars and registrants, as well as for users of the Internet in general.

Afilias defines abusive use as the wrong or excessive use of power, position or ability, and includes, without limitation, the following:

- **Illegal or fraudulent actions;**
- **Spam**: The use of electronic messaging systems to send unsolicited bulk messages. The term applies to e-mail spam and similar abuses such as instant messaging spam, mobile messaging spam, and the spamming of Web sites and Internet forums. An example, for purposes of illustration, would be the use of e-mail in denial-of-service attacks;
- **Phishing**: The use of counterfeit Web pages that are designed to trick recipients into divulging sensitive data such as usernames, passwords, or financial data;
- **Pharming**: The redirecting of unknowing users to fraudulent sites or services, typically through DNS hijacking or poisoning;

- **Willful distribution of malware**: The dissemination of software designed to infiltrate or damage a computer system without the owner's informed consent. Examples include, without limitation, computer viruses, worms, keyloggers, and trojan horses;
- **Fast flux hosting**: Use of fast-flux techniques to disguise the location of Web sites or other Internet services, or to avoid detection and mitigation efforts, or to host illegal activities. Fast-flux techniques use DNS to frequently change the location on the Internet to which the domain name of an Internet host or name server resolves. Fast flux hosting may be used only with prior permission of Afilias.
- **Botnet command and control**: Services run on a domain name that are used to control a collection of compromised computers or "zombies," or to direct denial-of-service attacks (DDoS attacks);
- **Distribution of child pornography; and**
- **Illegal Access to Other Computers or Networks**: Illegally accessing computers, accounts, or networks belonging to another party, or attempting to penetrate security measures of another individual's system (often known as "hacking"). Also, any activity that might be used as a precursor to an attempted system penetration (e.g., port scan, stealth scan, or other information gathering activity).

Registrars shall promptly investigate complaints alleging any such abusive practices, and shall take all appropriate actions based upon such investigations. Further, Registrar shall comply promptly with any commercially reasonable requests or recommendations with respect to such abusive practices made by Registry Operator or any competent legal authority.

Pursuant to Section 3.6.5 of the RRA, Afilias reserves the right to deny, cancel or transfer any registration or transaction, or place any domain name(s) on registry lock, hold or similar status, that it deems necessary, in its discretion; (1) to protect the integrity and stability of the registry; (2) to comply with any applicable laws, government rules or requirements, requests of law enforcement, or any dispute resolution process; (3) to avoid any liability, civil or criminal, on the part of Afilias, as well as its affiliates, subsidiaries, officers, directors, and employees; (4) per the terms of the registration agreement or (5) to correct mistakes made by Afilias or any Registrar in connection with a domain name registration. Afilias also reserves the right to place upon registry lock, hold or similar status a domain name during resolution of a dispute. Abusive uses, as defined above, undertaken with respect to .INFO domain names shall give rise to the right of Afilias to take such actions under Section 3.6.5 of the RRA in its sole discretion.

****

Consultation

Please describe with specificity your consultations with the community, experts and or others. What were the quantity, nature and content of the consultations?

See below.

a. ***If the registry is a sponsored TLD, what were the nature and content of these consultations with the sponsored TLD community?***

Not Applicable

b. Were consultations with gTLD registrars or the registrar constituency appropriate? Which registrars were consulted? What were the nature and content of the consultation?

Over the past six months, Afilias has worked cooperatively with the staff of more than 35 .INFO registrars with regard to issues surrounding abusive uses of .INFO domain names.. Those 35 registrars sponsor more than 85% of the domains under management in the .INFO registry. This program evaluated practices for reporting and mitigating abusive domain names. The process included in-depth conversations with the compliance staff at several large registrars in order to understand their anti-abuse policies and processes, since those registrars deal with abuse issues on a regular basis. (Some of the registrars we spoke with were GoDaddy, MarkMonitor, MelbourneIT, Tucows, and DirectI/PublicDomainRegistry.com.) The outreach efforts resulted in the 35 registrars suspending more than 50,000 .INFO domains that were being used for abusive purposes.

We found that registrar practices, response capabilities and response times vary widely. While a few of the registrars with which we consulted maintain dedicated, staffed abuse desks, most do not. While many registrars were very cooperative in pursuing the goals of this program, a few were less so, and some were unresponsive.

On June 20, 2008 Afilias e-mailed the first draft of the policy to all accredited .INFO registrars.

As a part of the ICANN Meeting in Paris in June 2008, Afilias presented salient aspects of the proposed policy to the Registrar Constituency. Members from the Registrar Constituency provided feedback on the proposed policy. Based upon this consultation with the Registrar Constituency members, Afilias has revised its proposed policy to remove from its definition of abusive uses the section titled “Other abusive behaviors”, which had drawn comments regarding breadth of scope, as well as removing the sentence regarding breach.

Were consultations with other constituency groups appropriate? Which groups were consulted? What were the nature and content of these consultations?

Afilias consulted with several eminent outside Internet security experts, who advised us on emerging threats and best practices. For instance, over the past six months, Afilias had conversations with John Klensin (independent consultant), Dave Piscitello (Principal, CoreComm) and Steve Crocker (Chairman, ICANN SSAC). We have incorporated comments and/or modifications suggested by these individuals into this policy. We intend to send a copy of the policy document to the ICANN SSAC in the near future.

In addition, Afilias is a member of the steering committee of the Anti-Phishing Working Group (APWG), and has consulted with a number of its members regarding anti-abuse issues and mitigation practices. The APWG is the global pan-industrial and law enforcement association focused on eliminating fraud and identity theft that result from phishing, pharming, and e-mail spoofing of all types. The APWG also focuses on policy-related issues associated with the Domain Name System (DNS) to examine abuses of the DNS that may require remediation. Afilias staff co-authored two major APWG research papers. One was the most comprehensive study to date of how domain names are being used for phishing, and the techniques that phishers are using to register and abuse domain names. This data-intensive, fact-based study provided a number of detection and mitigation strategies for the domain name industry. (http://www.apwg.org/reports/APWG_GlobalPhishingSurvey2007.pdf). The other paper studied whether there was a relationship between phishing and domain tasting. That report was created to advise ICANN's GNSO and was referenced in the"GNSO Final Report on Domain Tasting."

Further, Afilias is a founding member of the Registry Internet Safety Group (RISG). The purpose of the group is to facilitate dialogue, affect change, and promulgate best practices to combat domain name abuse, Internet identity theft in all its forms, and malware distribution. The member registry operators are examining anti-abuse best practices and use cases for registries, and opportunities for data sharing.

Afilias has been consulting with law enforcement, including agents from the U.S. Federal Bureau of Investigation who are responsible for investigating cybercrime.

During the formulation of this registry policy proposal, Afilias engaged in a collaborative dialog with representative individuals from within the business, intellectual property, and non-commercial communities. The need to combat illegal domain name use is well-known and is not controversial.

Were consultations with end users appropriate? Which groups were consulted? What were the nature and content of these consultations?

Afilias received input from victims of cyber-crime and mitigation experts who represent them. These include frequent targets of phishing and malware. Agents from the U.S. Federal Bureau of Investigation provided input regarding the impact of cyber-crime.

As a registry operator, Afilias does not usually have contact with the registrants of .INFO domains, since such contact is traditionally conducted through their registrars. We do know that, as a result of the efforts of Afilias to provide reports and intelligence to registrars, Afilias has aided several hundred end-users who had their Web sites compromised by professional phishers.

c. Who would endorse the introduction of this service? What were the nature and content of these consultations?

Numerous registrars have expressed interest in Afilias' anti-abuse efforts thus far. They have stated that registry efforts help them discover domain name abuse and thereby protect end users and registrants. Registrars have also told us that abuse cases cost them hundreds to thousands of dollars each, when customer service and credit-card chargeback costs are factored in. These registrars are interested in avoiding those problems by using intelligence supplied by the registry.

We have received thanks for our efforts from personnel at major online companies such as Microsoft, international banks, Google, and PayPal. These companies and their end-users bear much of the brunt of online crime that leverages domain names.

Law enforcement personnel have asked us to mitigate domain name use, and have welcomed our proactive outreach efforts.

The Anti-Phishing Working Group is generally encouraging registry operators to adopt anti-abuse programs.

In summary, business, intellectual property, the registry, registrars, law enforcement, and end-users will benefit from the new policy. While Afilias cannot attest here that the above parties formally "endorse" this submission, we believe that the proposal is a welcome and constructive step forward to addressing pressing problems.

d. Who would object to the introduction of this service? What were (or would be) the nature and content of these consultations?

Parties who use domain names for abusive or illegal purposes, and parties who sell services to such abusers, may object to the new policy.

Some registrars may be concerned that the new policy will create more work from them. We do not believe that the new policy will substantially affect the way we have worked with most registrars. Our continuing approach is to work with and through our registrars in a collaborative fashion. We do expect registrars to respond to and follow up on our abuse reports. We believe that registrars share our view that organizations that are part of the infrastructure of the Internet (including registries, registrars, hosting providers, and ISPs) should all take reasonable steps to protect against online abuse and crime, in order to fulfill their obligations to protect the stability and security of the Internet.

Timeline

In accordance with the provisions of section 3.5.2 of the .INFO RRA, the policy will take effect upon thirty (30) days notice to the .INFO registrars.

Business Description

Describe how the Proposed Service will be offered:

The policy will be implemented according to its terms, as detailed above.

Describe quality assurance plan or testing of Proposed Service:

We intend to apply this policy only after careful scrutiny of each case, and a review of the supporting evidence for abusive practices. Specifically, requests for action from registrars will be accompanied by supporting documentation which demonstrates the need for expedited action to be taken by the registrar. This approach conforms to industry best-practices regarding the ability of potentially affected registrars to provide relevant information prior to an enforcement action.

Please list any relevant RFCs or White Papers on the proposed service and explain how those papers are relevant.

Afilias is not aware of any relevant RFC or directly relevant White Papers.

Contractual Provisions

List the relevant contractual provisions impacted by the Proposed Service:

The Policy will be adopted pursuant to section 3.5.2 of the .INFO RRA.

What effect, if any, will the Proposed Service have on the reporting of data to ICANN?

None

What effect, if any, will the Proposed Service have on Whois?

None.

What effect, if any, will the proposed service have on the price of a domain name registration?

None.

Contract Amendments

Please describe or provide the necessary contractual amendments for the proposed service:

The Policy will be adopted pursuant to section 3.5.2 of the .INFO RRA. No amendment to any contract is required.

Benefits of Service

Describe the benefits of the Proposed Service:

The policy has several obvious beneficial effects, including:

- It will help domain name registrants. For example, some phishing takes place on compromised or hacked machines, and registrants are usually not be aware that their sites have been altered until they are notified via outreach.
- The policy will make it more difficult for criminals to use domain names for illegal purposes.
- The policy will help registrars identify problem registrants.
- It will benefit end-users by making the Internet a safer and more trustworthy place.
- Overall, the policy will allow more abusive domain name uses to be mitigated, and will decrease the up-times of related Web sites.

Competition

Do you believe your proposed new Registry Service would have any positive or negative effects on competition? If so, please explain:

Afilias does not believe that the implementation of the policy will have a significant effect on competition.

How would you define the markets in which your proposed Registry Service would compete?

Not applicable.

What companies/entities provide services or products that are similar in substance or effect to your proposed Registry Service?

ICANN-accredited registrars are free to craft anti-abuse policies for inclusion in their Registrar-Registrant agreements. Those Registrar-Registrant agreements routinely forbid the illegal use of domain names, and often address many of the specific abusive practices in the registry policy that Afilias proposes.

Other registries have relevant policies. For example, ICANN's contract with the .BIZ registry operator includes a prohibition against registrants "Using the domain name for the submission of unsolicited bulk e-mail, phishing, pharming or other abusive or fraudulent purposes." < http://www.icann.org/tlds/agreements/biz/appendix-08-08dec06.htm>

Please note that the vast majority of domain name-related abuses and crimes are not mitigated by the efforts of law enforcement. Domain and site take-downs are usually accomplished through the efforts of third parties such as the companies being targeted by the criminals, private security companies, ISPs, hosting companies, registrars, registries, and individual users.

In view of your status as a registry operator, would the introduction of your proposed Registry Service potentially impair the ability of other companies/entities that provide similar products or services to compete?

Afilias does not believe that its proposed service would negatively impair the ability of other companies/entities that provide similar services to compete.

Do you propose to work with a vendor or contractor to provide the proposed Registry Service? If so, what is the name of the vendor/contractor, and describe the nature of the services the vendor/contractor would provide.

Afilias does not anticipate using any vendor or contractor to implement the proposed policy.

Have you communicated with any of the entities whose products or services might be affected by the introduction of your proposed Registry Service? If so, please describe the communications.

See the prior sections of this application regarding consultations with third parties.

Do you have any documents that address the possible effects on competition of your proposed Registry Service? If so, please submit them with your application. (ICANN will keep the documents confidential).

None.

Security and Stability

Does the proposed service alter the storage and input of Registry Data?

No.

Please explain how the proposed service will affect the throughput, response time, consistency or coherence of responses to Internet servers or end systems:

Afilias anticipates no impact on the throughput, response time, consistency of coherence of responses to Internet servers of end systems.

Have technical concerns been raised about the proposed service, and if so, how do you intend to address those concerns?

Afilias is not aware of any technical concerns regarding the proposed service.

Other Issues

Are there any Intellectual Property considerations raised by the Proposed Service?

No.

Does the proposed service contain intellectual property exclusive to your gTLD registry?

No

List Disclaimers provided to potential customers regarding the Proposed Service:

None.

Any other relevant information to include with this request:

None