First-round constituency input template
Version August 7, 2008

Registry Constituency Input Template:

Fast-Flux Working Group

The GNSO Council has formed a Working Group of interested stakeholders and Constituency representatives, to collaborate broadly with knowledgeable individuals and organizations, in order to develop potential policy options to curtail the criminal use of fast flux hosting.

An early part of the working group's effort will incorporate ideas and suggestions gathered from Constituencies. View this as a brainstorming effort, rather than a formal policy-comment process (a formal Constituency Statement process is scheduled to start about a month from now). Our goal at this stage is to allow very broad participation in our drafting effort. So there is no requirement that your Constituency provide any suggestions at this time -- but any ideas are welcome.

Inserting your Constituency's response in this form will make it much easier for the Working Group to summarize the Constituency responses. This information is helpful to the community in understanding the points of view of various stakeholders.

Please identify the members of your constituency who participated in developing the perspective(s) set forth below:

Voting in favor of this document, in full (listed alphabetically by TLD): NeuStar (.BIZ), puntCAT (.CAT), VeriSign (.COM, .NET), DotCooperation LLC (.COOP), Afilias (.INFO), Employ Media (.JOBS), mTLD (.MOBI), Global Name Registry (.NAME), Public Interest Registry (.ORG), RegistryPro (.PRO). Voting against: none. Abstaining: none. Absent/no response: SITA (.AERO), dotAsia Organisation (.ASIA), MuseDoma (.MUSEUM), TelNIC (.TEL), Tralliance Corp. (.TRAVEL).

Please describe the process by which your constituency arrived at the perspective(s) set forth below:

Based upon discussion of the issues, Registry Constituency members created a draft document, which was then circulated amongst all Constituency members for rounds of discussion and editing. Further discussion took place in two constituency teleconferences. After several iterations, a final draft was voted upon.

NOTE: Consensus is not required at this stage of the process. If ideas differ within the Constituency, please provide all of them. The working group will work to resolve the differences and the Constituency will have an opportunity to comment in the formal Constituency Statement process.

Executive Summary:

The Registry Constituency recognizes that fast-flux hosting is used by criminals to perpetrate a variety of illegal activities, which harm a variety of parties including registry operators. The

Constituency supports further discussion of voluntary best practices that would facilitate data sharing and are designed to identify problematic domain names.

The Registry Constituency feels that key issues are outside of ICANN's purview, and beyond the scope of GNSO policy-making:

1. ICANN's purview with regard to making policy to mitigate criminal use of the DNS is very limited, and technical. At the core, combating fast-flux hosting is a matter of identifying and disabling domains that are being used for illegal purposes.
2. It is not within ICANN's purview to place gTLD registries in a position to become extensions of law enforcement regimes around the world, by requiring registries to take action against a domain name that may be in violation of one or more nation's laws. In addition, it is not within ICANN's purview to determine (or license another evaluative body to determine) which domain names are being used for illegal purposes.
3. To require registries to act against certain domain names may also expose registries to unknown liabilities, and it is not clear whether ICANN has an effective ability to protect contracting parties from these liabilities.
4. Contracted parties should have the ability to set relevant terms of service for their respective TLDs or registrar service, as applicable. Various parties already have the ability to act against problematic domain names, according to their various contracts and terms of service. Models for this activity already exist in directly relevant areas, and fast-flux domains are already being taken down. Every day, members of the Internet community – including hosting providers, network operators, registrars, registries, businesses and intellectual property owners, and law enforcement bodies—deal with domain names used for phishing, spam, malware, and other problems. Such problems have been resolved without involving ICANN, and we believe that most proposed solutions to deal with fast-flux hosting should not involve ICANN intervention.
5. There are venues for dealing with criminal activity, but ICANN is not such a venue. Criminals adapt their tactics quickly, and the parties taking action against them should be free to craft their own solutions as conditions suggest.
6. We do not believe that the Working Group has yet demonstrated, from a technical standpoint, that fast-flux hosting has materially impacted the interoperability, technical reliability, and/or operational stability of Registrar Services, Registry Services, the DNS, or the Internet. These continue to function well.
7. We believe that as of the date of this statement, the Working Group has not adequately quantified the scope of the problem based upon data. It is therefore difficult to evaluate the costs/benefits of solutions.

The Registry Constituency also explains below why it feels that some proposed solutions:

1. are technically and legally outside the power of registries to implement,
2. present significant engineering issues that could require revisions to protocols and the DNS itself,
3. are not relevant to some registries, and
4. could negatively impact various parties, some of which may be using fast-flux techniques for legitimate purposes.

Questions:

1. Who benefits from fast flux, and who is harmed?

Phishing, pharming, spam, and other illegal activities that may be perpetrated through the use of fast-flux networks represent a well-known threat to the security of Internet users.

These types of domain name abuses can also harm the reputations and brands of specific TLDs. TLDs can be saddled with negative reputations for higher-than-average abuse rates. Some registries have adopted voluntary means to help address these issues. Most registries have no direct relationship with the registrants responsible for the abusive behavior.

2. Who would benefit from cessation of the practice and who would be harmed?

We will use the definitions found in the *GNSO Issues Report on Fast Flux Hosting*, which are:

- Fast Flux: In this context, the term “fast flux” refers to rapid and repeated changes to A and/or NS resource records in a DNS zone, which have the effect of rapidly changing the location (IP address) to which the domain name of an Internet host (A) or name server (NS) resolves.
- Fast Flux Hosting: The practice of using fast flux techniques to disguise the location of web sites or other Internet services that host illegal activities.

Using these definitions, “fast flux” is a technique or technical implementation, while “fast flux hosting” is the use of the technique for criminal purposes.

We are concerned that solutions aimed at certain types of nefarious activities criminal activity could prohibit or constrain legitimate activities that uses similar techniques, or might not accurately interpret the intent of the activity. It may be difficult to distinguish some criminal uses from non-criminal uses, especially using technical means only.

We are also concerned that cessation of fast-flux could impede the creation of new and legitimate services on the Internet, and we would like to know whether the cessation of fast-flux would impact any existing services, for example commercial services or services that facilitate speech on the Internet. As noted in its bylaws, one of ICANN’s core values is “Respecting the creativity, innovation, and flow of information made possible by the Internet.”

3. Are registry operators involved, or could they be, in fast flux hosting activities? If so, how?

Some TLDs probably have never had domains that operate on fast-flux networks, and are less vulnerable. Fast-flux domains used for nefarious purposes are registered by criminals, who may not have easy access to domains in certain sTLDs. Some solutions might therefore not be good fits for all registries, and voluntary participation to best practices and/or specific programs might therefore be more viable.

Fast-flux hosting can be addressed if the domain names involved are not allowed to resolve. Domain names are stopped from resolving by removing them from the zone (by placing an EPP HOLD status, or removing the associated nameservers from the domain record, or by deleting the name from the registry.) Two parties have the technical ability to remove a domain name from the TLD zone – the sponsoring registrar, or the registry operator. (Registrants and resellers act through a registrar’s system.) The relevant hosting provider(s) also have the ability to stop a domain name from functioning, by making changes at the nameservers.

ICANN’s agreements with gTLD registry operators give registry operators varying rights to suspend domain names. Registrars, on the other hand, have direct contractual relationships with their registrants, and are often in a better position to communicate directly with their customers. (See Question #4 below for more.) Therefore, registries have often adopted practices to present abuse reports to the registrar of record.

As per its bylaws, the mission of ICANN is to "coordinate, at the overall level, the global Internet's systems of unique identifiers, and in particular to ensure the stable and secure operation of the Internet's unique identifier systems," and ICANN "coordinates policy development reasonably and appropriately related to these technical functions." We do not think that making policy to mitigate criminal use of fast-flux hosting is reasonably and appropriately related to ICANN's technical functions. At the core, combating fast-flux hosting is a matter of identifying and disabling domains that are being used for illegal purposes.

It is not within ICANN's purview to require registries to become an arm of a law enforcement regime, nor to act on every allegation that may be made about purported illegal uses of domain names. It is not within ICANN's purview to determine (or license another evaluative body to determine), which domain names are being used for illegal purposes. To require registries to act against certain domain names may also expose registries to unknown liabilities, and it is not clear whether ICANN has an effective ability to protect contracting parties from these liabilities.

The *GNSO Issues Report on Fast Flux Hosting* stated: "The community of researchers, system administrators, law enforcement officials, and consumer advocates who are fighting Internet scams that are enabled or accelerated by fast flux hosting have concluded that trying to thwart fast flux hosting by detecting and dismantling the botnets (fast flux service networks) is not effective." We agree. However, the *Issues Report* then went on to say: "Other measures that require the cooperation of DNS registries and registrars to identify or defeat fast flux techniques are expected to be much more effective." And that "ICANN Staff research has confirmed that fast flux hosting…. could be significantly curtailed by changes in the way in which DNS registries and registrars currently operate." (page 10)

We believe that those statements, especially relating to registries, are overbroad and need careful examination. Some of the proposed solutions involving registries are impossible for registries to implement, or will be ineffective for technical reasons. For example, registries have no role in how many fast-flux networks operate, registries are not necessarily privileged in their ability to detect fast-flux domains, and registries have differing abilities to act directly against abusive uses of domain names.

Please see response to Question 7 below for more commentary on technical and policy solutions that may involve registries. The Registry Constituency is interested in addressing, with the wider community, the problems caused by fast-flux hosting.

4. Are registrars involved in fast flux hosting activities? If so, how?

Fast-flux hosting can be addressed if the domain names involved are not allowed to resolve. As far as we are aware, all ICANN-accredited registrars have registrar-registrant contracts and terms of service that prohibit registrants from using their domain names for illegal or abusive purposes. These contracts allow registrars to variously suspend such domain names (i.e., stop them from resolving), delete them, and/or cancel the registrant's rights and/or control over the domain. The agreements usually require the registrants to indemnify the registrars as well. Registrars are free to enforce their terms of service, and exercise these rights regularly by suspending many gTLD domain names each day for spam, phishing, malware distribution, the distribution of child pornography, and other abuses.

5. How are registrants affected by fast flux hosting?

6. How are Internet users affected by fast flux hosting?

7. What technical, e.g. changes to the way in which DNS updates operate, and policy, e.g. changes to registry/registrar agreements or rules governing permissible registrant behavior measures could be implemented by registries and registrars to mitigate the negative effects of fast flux?

It is important to understand the technical means available to TLD registries, including the relevant Internet specifications and protocols. Unfortunately, some proposed solutions to fast-flux hosting that involve registries are currently impossible, or would require significant revisions to DNS protocols, or would require significant upgrades in deployed resolver code. Other proposed solutions may have limited impact, or are not exclusive to registries only.

Beyond the technical issues, some proposed solutions would require wide-ranging changes to registration paradigms, registrant behavior, and registry business practices. These should be examined carefully. In all cases the benefits should be proven to outweigh the costs, and registries should be given the means to recover the costs associated with any solutions imposed upon them.

Network operators, businesses, hosting providers, government organizations, intellectual property owners, registries, and registrars all have roles to play when addressing various Internet abuses, and collaborative solutions and data sharing may be useful.

Below are some assumptions and proposals about how registries may be involved in fast-flux hosting:

The *GNSO Issues Report on Fast Flux Hosting* [http://gnso.icann.org/issues/fast-flux-hosting/gnso-issues-report-fast-flux-25mar08.pdf] stated:

> Registries and registrars can curb the practice in two ways: (1) by monitoring DNS activity (fast flux is easy to detect) and reporting suspicious behavior to law enforcement or other appropriate reporting mechanism; and (2) by adopting measures that make fast flux either harder to perform or unattractive. Some possible measures that have been suggested include:
>
> - authenticating contacts before permitting changes to NS records;
> - preventing automated NS record changes;
> - enforcing a minimum “time to live” (TTL) for name server query responses;

> • limiting the number of name servers that can be defined for a given domain; and
> • limiting the number of address record (A) changes that can be made within a specified time interval to the name servers associated with a registered domain.
>
> (page 11)

The *SSAC Advisory on Fast Flux Hosting and DNS* [http://www.icann.org/en/committees/security/sac025.pdf] identified the following potential solutions that could possibly involve registries:

- Adopting procedures that accelerate the suspension of a domain name,
- Remove domains used in fast flux hosting from service
- Authenticate contacts before permitting changes to name server configurations.
- Implement measures to prevent automated (scripted) changes to name server configurations.
- Set a minimum allowed TTL (e.g., 30 minutes) that is long enough to thwart the double flux element of fast flux hosting.
- Separate "short TTL updates" from normal registration change processing.
- Implement or expand abuse monitoring systems to report excessive DNS configuration changes.
- Publish and enforce a Universal Terms of Service agreement that prohibits the use of a registered domain and hosting services (DNS, web, mail) to abet illegal or objectionable activities (as enumerated in the agreement).
- Rate-limit or (limit by number per hour/day/week) changes to name servers associated with a registered domain name.

Below we will examine these ideas and others; we find many of them problematic.

Do registries have any control over fast-flux networks?

Single-flux fast-flux networks do not involve changes to records in a TLD registry. Single-flux service networks change A records for their front-end node IP address. This happens at a level below the registry.

Therefore, registries and registrars have no control over single-flux networks. No registry records are changed, and registries cannot monitor or detect that change activity via registry data. A great deal of fast-flux hosting takes place on single-flux networks.

Double-flux fast-flux networks *do* involve changes to records in a TLD registry. Double-flux is where both the NS records (authoritative name server for the domain) and A records (Web serving host or hosts for the target) are regularly changed, making the fast-flux service network more dynamic. For double-flux techniques to work, the registrant must frequently change the NS information at the registry.

Registries could analyze registry records to find nameserver changes, but would have to couple them with a single-flux detection method in order to be meaningful.

We see the following additional issues:

1. Problematic changes (i.e., those done for criminal intent) must be distinguished from non-problematic updates. This is a non-trivial matter in a registry of any size. Domain name

registries are not in a position to interpret what does or does not constitute criminal activity in every legal jurisdiction in the world.

2. There is some evidence that some operators of double-flux networks change their nameserver records only on an infrequent basis. In some observed cases the interval between changes is days or even weeks. Such change rates do not qualify as rapid, and some so-called double-flux networks might not be worthy of the name.
3. There are many legitimate reasons why a registrant would want to change nameserver records more than twice or three times in the course of a month. Restrictions on change rates at such levels would unnecessarily restrict normal operations and user freedom.
4. Changes at the TLD level are detectable to anyone analyzing the TLD zone files, which are available daily free of charge.
5. Since changes to TLD records are relatively easy for the registry operator and other observers to detect, they might not be attractive methods for criminals.
6. By themselves, registry records give an incomplete picture in other ways. Registry operators cannot see some hosting-related changes because they involve changes to registry records in *other* TLDs. A registry's records can reveal when the IP of a nameserver object is changed – but *only* if the nameserver exists on a domain in that TLD. For example, the nameserver ns1.example.com exists as a record in the .COM registry, and that nameserver record must have an IP address associated with it, because the .COM registry is authoritative for .COM objects. The nameserver ns1.example.com may also exist as an object in the .ORG registry as well. However, that nameserver record in the .ORG registry cannot have an IP address associated with it, because the .COM registry is authoritative for .COM objects. This means that the .ORG registry operator cannot use its registry records to see if the IP of ns1.example.com is changing.

There is a need for more data to understand how many fast-flux networks operate on single flux versus double flux, at what rates double flux networks change their nameserver records in registries, and how frequent such changes need to be in order for a network to be considered a double-flux network. At this time there is not enough data to establish the scope of the problem.

Are registries in a special position to detect fast-flux hosting?

No. Fast-flux hosting is most commonly detected by querying nameservers for A records and recording the changes to those records over time. This method requires basic tools, and is currently practiced by many entities, including security companies, network operators, and academic researchers. Most subscribe to the gTLD zone files, which ICANN requires the registries to make available free of charge.

Some registry operators may be able to analyze DNS query data that comes to the TLD servers. This data is voluminous in larger TLDs, and is harder to interpret.

Is fast-flux hosting easy to detect, or easy to positively identify? Is it easy to identify criminal behavior?

The answers to all these questions is "no." While it is easy to compile query data in the way described above, that data must then be interpreted. The key concept is that the observer must be able to separate out criminal uses of the fast flux technique from non-criminal uses, and in some cases this can be very difficult.

Some believe that fast flux hosting can easily be identified on an automated basis. But automated checking is not accurate when determining the criminal intent of any particular implementation. Rather, it may be possible for a certain percentage of criminal fast-flux hosting to be identified to a high degree of accuracy. This means that some criminal fast-flux hosting may be overlooked or discarded because it does not pass enough "tests" of bad intent, that manual checking is advisable, and that false positives will probably never be eliminated.

These problems are important, because the ultimate goal may be to suspend the resolution of fast-flux domain names. Parties who suspend domain names must perform due diligence, and are exposed to liability.

The Working Group has also examined case studies that demonstrate that:

1. fast-flux detection systems create false-positives.
2. It is not always possible to determine the intent that some fast-flux domains are being used for.
3. It is not always possible to determine whether the hosts involved are compromised.

Improved information availability may be useful for combating fast flux, but will result in incremental improvements only, just as blacklists and antivirus products have produced incremental progress against spam, phishing, and malware.

Can TLD registries control TTL values?

No, not in a way that is meaningful to this problem. Practically, domain name users and their hosting providers are in control of the TTLs related to their domain names, and are free to set whatever TTL they like.

Registrars have no mechanism by which they can set the TTL on records in the parent zone for domains they register, and registrars do not set or populate the time-to-live (TTL) for the resource records found in TLD zone files.

TLD registries may set a default TTL value. However, this TTL value is a default value only and does not control the actual TTLs associated with names in the zone. Instead, a TTL is set by the authoritative nameserver for a particular resource record. The authoritative data for a zone is below the zone cut, and any registry operator has a limited to no influence on the TTL on a delegation.

For example, any long TTL specified in the .COM zone in the NS set for a domain would be overwritten in resolvers' caches by the TTL specified in the daughter zone, which the registry does not host. So if the .COM registry operator sets a TTL of 600 minutes, and whoever hosts the individual domain name sets a TTL of 3 seconds, what gets cached is 3 seconds.

So, this default TTL has no practical impact on fast-flux hosting, because domain name registrants and their hosting providers are ultimately in control of the authoritative TTLs, and are free to set whatever TTL they like. This user-set value is the TTL value that prevails on the Internet, and this is a current, designed feature of the DNS. We do not know of any mechanism by which ICANN could limit the TTLs that zone administrators decide to install on their own RRsets.

Note that the EPP registry-registrar protocol offers no mechanism for registrars to specify TTL values to the registry.

What are the effects of either short or long TTLs on NS sets above the zone cut for queries which follow those delegations? This is not well understood. It is not known, for example, if increasing the TTL on NS sets in TLD zones could have an effect on some caches across the Internet. Before ICANN makes any related policy, we would expect ICANN to commission a credible technical study, and there should be significant input from the IETF.

Any proposed changes to the DNS protocols, or to their standard implementations, should have the support of the engineering community, and such discussions should involve a formal consultative process with the IETF.

Are there legitimate uses for short TTLs?

Yes. Any entity that operates a Web site or other Internet service has legitimate reasons for using short TTLs, at least for finite periods of time. Such uses are written into relevant RFCs, including the domain name RFCs 1034 and 1035. Internet services that are subject to a high change frequency legitimately use low TTLs, and even TTLs of zero. Uses of zero-length TTLs are mentioned in relevant RFCs, including RFC 1035.

Imposing minimum lengths for TTLs is therefore contrary to standard engineering practices, will interfere with the operation of existing sites and services, may stifle the development of innovative services, and will impose costs on site operators and their service providers. Even if such limits were desired, there is presently no practical way that any entity could impose minimum TTLs on those parties responsible for setting them authoritatively. We do not know of any technical mechanism by which ICANN could limit the TTLs that zone administrators decide to install on their own RRsets. Any policy mechanism to limit the TTLs that zone administrators decide to install on their own RRsets would require volunteer compliance from all hosting parties world-wide -- which will not be practical or effective.

Is it practical or desirable to implement measures that limit the number of nameserver changes allowed in a given time period, or prevent automated (scripted) changes to name server configurations? Would authenticating contacts before permitting changes to NS records be practical or desirable?

Such a solution would force registrants to change their behaviors and expectations, and would impose delays and inconveniences upon Web site managers. The current paradigm allows gTLD registrants to change their records as they see fit, and it would be difficult to roll this back.

Such a system would also impose additional costs on registrars, which could be passed on to registrants in the form of higher registration fees.

As noted above, these counter-measures are effective against double-flux networks only, and the use of double-flux networks should be quantified so as to understand the impact of the proposed solution and weigh the benefits against the costs.

Is limiting the number of name servers that can be defined for a given domain practical or desirable?

No. Fast-fluxing domain names usually only have a few nameservers associated with them, often only four or five. There are legitimate reasons for registrants to use that number of nameservers, including robustness and redundancy. An example is icann.org, which has five nameservers listed.

Is reporting to law enforcement useful and effective?

We applaud the dedicated work of law enforcement, and encourage reporting, but it does not provide a comprehensive or speedy solution. Counter to some popular perception, the vast majority of Internet crime is not addressed through the efforts of law enforcement, and is not reported to law enforcement. Domain take-downs are usually accomplished by the entities affected, working with ISPs, hosting companies, server operators, registrars, registries, and individual computer owners. Law enforcement bodies are often under-funded, and often do not have resources to devote to cyber-crime. Jurisdictional issues also hamper the investigation and prosecution of Internet crimes. Some registries and registrars have established relationships with law enforcement bodies to provide information related to nefarious uses of domain names.

8. What would be the impact (positive or negative) of establishing limitations, guidelines, or restrictions on registrants, registrars and/or registries with respect to practices that enable or facilitate fast flux hosting? What would be the impact of these limitations, guidelines, or restrictions to product and service innovation?

Also see number 7 above for discussions of the applicability and impact of establishing limitations, guidelines, or restrictions on those parties.

Some solutions aimed at criminal activity could prohibit or constrain non-criminal activity that use similar techniques, or might not differentiate adequately based on the intent of the activity. Other solutions may require parties to separate the criminal uses from the non-criminal, which is sometimes difficult. Whether solutions to criminal fast-flux may constrain non-criminal services and/or the creation of new and legitimate services on the Internet are pertinent issues for consideration. See also #7 above. One case study examined by the Working Group indicates the possible existence of such a service (UltraReach, which claims to be an anti-censorship service founded under human rights repression).   The Working Group does not know how many relevant sites or services may already be operating on the Internet, or what they do, and therefore does not know the impact of some potential solutions. Absent such knowledge, we think it wise to “do no harm” and avoid limitations, guidelines, or restrictions that could impact legitimate services.

We also note that fast flux hosting is a phenomenon that utilizes the DNS, and therefore is technically relevant to all TLDs. Fast flux hosting currently occurs on many domain names and hosts across a wide range of TLDs.   Regulation in the gTLD space only would leave fast flux activity unaddressed in the ccTLD space. We ask whether there is lasting value to developing gTLD policy regarding any issue that occurs in both gTLDs and ccTLDs.

Attempts to technically (rather than administratively) cope with fast flux may result in increasingly complicated solutions that may inadvertently impact innocent parties, and/or may or break the network in hard-to-diagnose ways.

9. What are some of the best practices available with regard to protection from fast flux?

It may be useful to look at fast flux as an example of a generalized problem: domain name abuse. In many ways, fast-flux hosting is not conceptually any different from other domain name abuses. Spam, phishing, pharming, and malware also all take advantage of the DNS and Internet protocols. Efforts to mitigate these problems involve detection of potential problem domains, determinations of whether the activities on specific domain names may be illegal or violate terms of service, and then mitigation work. These are many of the exact same issues faced in the current fight against fast-flux hosting, and best practices for domain name takedowns could be adapted. In fact, fast-flux domains are already being mitigated using these existing practices.

Those problems are mitigated on a daily basis by private parties, including ISPs and network operators, hosting companies, registrars, registries, security companies, law enforcement, and individuals. This community is free to adapt its tactics and invent new alliances as needed. We recall that one of ICANN's core values, enshrined in its bylaws, is: "To the extent feasible and appropriate, delegating coordination functions to or recognizing the policy role of other responsible entities that reflect the interests of affected parties."

There are cooperative initiatives designed to facilitate data sharing and the identification of problematic domain names. Examples include the Anti-Phishing Working Group (APWG) for phishing and identity theft, the Messaging Anti-Abuse Working Group (MAAWG) for spam, ShadowServer Foundation for botnets, StopBadware.org for malware, and so on. Such efforts are a possible model for addressing fast-flux hosting.

See also #10 below.

10. Which areas of fast flux are in scope and out of scope for GNSO policy making?

The *GNSO Issues Report on Fast Flux Hosting* noted that a consensus policy resulting from the GNSO policy-development process would only be applicable if fast flux hosting is an issue "for which uniform or coordinated resolution is reasonably necessary to facilitate interoperability, technical reliability, and/or operational stability of Registrar Services, Registry Services, the DNS, or the Internet." While fast-flux hosting is a recognized problem that impacts various parties, fast-flux hosting has not materially impacted the interoperability, technical reliability, and/or operational stability of Registrar Services, Registry Services, the DNS, or the Internet. Those services continue to function in a stable and reliable manner.

As we have stated before, we believe that ICANN's purview with regard to making policy to mitigate criminal use of the DNS is very limited. At the core, combating fast-flux hosting is a matter of identifying and disabling domains that are being used for illegal purposes. It is not within ICANN's purview to impose requirements that registries act as judge and jury, or to act on every allegation that may be made about purported illegal uses of domain names. To do so would turn registries into enforcement agencies. It is not within ICANN's purview to determine (or license another evaluative body to determine), which domain names are being used for illegal purposes. To require registries to act against certain domain names may also expose registries to unknown liabilities, and it is not clear whether ICANN has an effective ability to protect contracting parties from these liabilities.

As per the *GNSO Issues Report on Fast Flux Hosting,* “General Counsel further notes that the overall question of how to mitigate the use of fast flux hosting for cybercrime is broader than the GNSO policy development process.” We agree. How to mitigate or prevent the use of fast-flux hosting for crime is indeed the central issue.

Efforts within ICANN and the GNSO will yield only incremental results. ICANN policies related to fast-flux hosting would only be applicable to gTLD registries and registrars. ccTLD domain names are also used for fast-flux hosting, which comprise almost half of the domain names on the Internet. Criminals who use fast-flux hosting could simply avoid the effects of ICANN policy by using ccTLD domain names. Therefore, we are unsure of the "lasting value" to developing gTLD policy regarding this issue. ICANN policies that target fast-flux hosting would only be applicable to gTLD registries and could impact their costs, and therefore affect their competitiveness with ccTLDs.

The *GNSO Issues Report on Fast Flux Hosting* stated that “The question of whether policy options would have ‘lasting value or applicability’ is a particularly important consideration in the context of fast flux hosting, where new static rules imposed through a policy development process might be quickly undermined by intrepid cybercriminals.” There are venues for dealing with criminal activity, and ICANN is not such a venue. ICANN is not suited to creating or overseeing detailed policies and procedures in such a rapidly evolving environment as cybercrime, where the criminals and responders are continually employing new measures and counter-measures. Instead, it may be more helpful to let private actors have the freedom and power to act within relevant legal and contractual contexts.

Spam, phishing, pharming, and malware are threats at least as prominent as fast-flux hosting, and arguably cause more damage and problems. Those abuses also leverage the DNS, have not entailed policy-making at the ICANN level, and have not demanded uniform or coordinated resolution. We therefore question why fast-flux hosting is a suitable topic for an ICANN process.

In many ways, fast-flux hosting is not conceptually any different from other domain name abuses. Spam, phishing, pharming, and malware also all take advantage of the DNS and Internet protocols. Those problems are mitigated on a daily basis by private parties, including ISPs and network operators, hosting companies, registrars, registries, security companies, and individuals. (Counter to some popular perception, the vast majority of abusive domain names are not taken down by the efforts of law enforcement.) These mitigation efforts often involve detection of potential problem sites, determinations of whether the activities on specific domain names are illegal or not, and then mitigation efforts. These are many of the exact same issues faced in the fight against fast-flux hosting. One of ICANN’s core values, enshrined in its bylaws, is: “To the extent feasible and appropriate, delegating coordination functions to or recognizing the policy role of other responsible entities that reflect the interests of affected parties.”