GAC Advice Response Form for Applicants

The Governmental Advisory Committee (GAC) has issued advice to the ICANN Board of Directors regarding New gTLD applications. Please see Section IV, Annex I, and Annex II of the GAC Beijing Communique for the full list of advice on individual strings, categories of strings, and strings that may warrant further GAC consideration.

Respondents should use this form to ensure their responses are appropriately tracked and routed to the ICANN Board for their consideration. Complete this form and submit it as an attachment to the ICANN Customer Service Center via your CSC Portal with the Subject, "[Application ID] Response to GAC Advice" (for example "1-111-11111 Response to GAC Advice"). All GAC Advice Responses must be received no later than 23:59:59 UTC on 10-May-2013.

Respondent:

Applicant Name	Vox Populi Registry Inc
Application ID	1-2080-92776
Applied for TLD (string)	sucks

Response:

TO: ICANN Board of Directors
FROM: John Berard, CEO, VoxPopuliRegistry
SUBJECT: Applicant .SUCKS response to GAC Beijing Communique
DATE: May 10, 2013

Vox Populi Registry Inc ("VoxPop") is pleased to provide detailed answers to the GAC Advice contained in the Beijing Communique issued on April 11, 2013. This response (attached to this cover note) is structured as follows:

Introduction

This provides a summary of our response

GAC Advise Response Details

This provides a detailed response to each of the 6 universal safeguards, the 5 safeguards applicable to Catgeory 1 strings as well as a response to the specific requirement of GAC Advice directed at the applicants for .SUCKS.

Annex

This provides a copy of our original Response to "Question 28: Abuse Prevention and Mitigation" to demonstrate to the ICANN Board that the measures being requested by the GAC have been inherent in our application since it was first filed.

It is this last point that is most important to VoxPop. This is now the third time that competing applicants will be given the opportunity to do the right thing which we saw as our responsibility at the start.

As the ICANN Board reviews our submission it will be clear that our application anticipated GAC requirements. We also expect that the ICANN Board will determine that the initial submission (and subsequent PIC submission) of the competing applications for .SUCKS do not and therefore should be disallowed under the rules of adherence to GAC Advice.

Regards
John Berard
CEO, Vox Populi Registry

Vox Populi Registry, Inc. response to GAC Advice contained in the Beijing Communique
May 19, 2013

- Introduction

Vox Populi Registry Inc ("VoxPop") is pleased to provide detailed answers to the GAC Advice requirements as requested in the GAC Beijing Communique, particularly as relates to the string-specific need to have a policy in place to address Cyber Bullying.

We include citations from our initial application for clarity and to demonstrate that it has been VoxPop's intention from the very beginning to operate .SUCKS with integrity, respect for the security and stability of the internet and with a view to providing a platform free of parking pages, pornography and any form of Cyber Bullying.

It is important to note that the VoxPop application is the ONLY application for .SUCKS to have had policies in place that specifically address the concerns detailed in the GAC Communique from our original submission. The competing applications for .SUCKS on the other hand, have not articulated any policy related to Cyber Bullying in any of their submissions.

It is also important to note that when the opportunity to offer a Public Interest Commitment arose, the other .SUCKS applicants did not act. Despite the issuance of GAC Early Warnings referencing Cyber Bullying, competing .SUCKS applications continued to remain silent in their intent to establish policies against Cyber Bullying.

On this basis alone, the ICANN Board should exercise it's right to reject the non-compliant competing applications for .SUCKS in favour of award to Vox Populi Registry on the simple basis that the competing applications have not addressed the GAC Communique and have ignored GAC Advice. Furthermore, to allow our competitors to make such a material change to their application at this stage of the process would be anti-competitive and would violate the intellectual property rights of our application, established by our original submission.

The remainder of this document provides a more detailed response to each of the GAC Communique concerns. VoxPop is confident the ICANN Board will evaluate our submission and concur that we meet and exceed the GAC requirements and we therefore look forward to moving ahead in the evaluation process.

- GAC Advice Response Details

With regards to the specific advice provided in the GAC Communique, the GAC first highlighted "six safeguards that should apply to all new gTLDs and be subject to contractual oversight".

1. The first safeguard is "WHOIS verification and checks"

A key part of enforcing legal behavior is deploying a WhoIs database that is accurate and accessible. Of course we will implement all elements of the new pending registry agreement (including adherence to the WHOIS ACCURACY PROGRAM SPECIFICATION and more general WHOIS SPECIFICATION), but it is our intention to mandate an even higher verification standard, with a focus on multiple elements, not just one or two.

In this way, should there be a question of performance in accordance with registry policies or local laws we can quickly connect legitimate inquiries to the registrant. As stated in our application, we seek to lead by example. Privacy and transparency are not mutually exclusive values; each is totally appropriate. So, too is accountability.

Our original response (Ref: 4.2.9 Promoting WhoIs Accuracy) provides the full detail of how we intend to achieve the goals of the current WHOIS specification. That response is provided here for clarity.

---start of original reponse snippet on WHOIS Accuracy

"4.2.9 Promoting WhoIs Accuracy
Inaccurate WhoIs information significantly hampers the ability to enforce policies in relation to abuse in the TLD by allowing the registrant to remain anonymous. In addition, LEAs rely on the integrity and accuracy of WhoIs information in their investigative processes to identify and locate wrongdoers. In recognition of this, we will implement a range of measures to promote the accuracy of WhoIs information in our TLD including:

– Random monthly audits: registrants of randomly selected domain names are contacted by telephone using the provided WhoIs information by a member of the ARI Abuse and Compliance Team in order to verify all WhoIs information. Where the registrant is not contactable by telephone, alternative contact details (email, postal address) will be used to contact the registrant, who must then provide a contact number that is verified by the member of the ARI Policy Compliance team. In the event that the registrant is not able to be contacted by any of the methods provided in WhoIs, the domain name will be cancelled following five contact attempts or one month after the initial contact attempt (based on the premise that a failure to respond is indicative of inaccurate WhoIs information and is grounds for terminating the registration agreement).

– Semi-annual audits: to identify incomplete WhoIs information. Registrants will be contacted using provided WhoIs information and requested to provide missing information. In the event that the registrant fails to provide missing information as requested, the domain name will be cancelled following five contact attempts or one month after the initial contact attempt.

– Email reminders: to update WhoIs information to be sent to registrants every 6 months.

– Reporting system: a web-based submission service for reporting WhoIs accuracy issues available on the Abuse page of our registry website.

– Analysis of registry data: to identify patterns and correlations indicative of inaccurate WhoIs (eg repetitive use of fraudulent details).

Registrants will continually be made aware, through the registry website and email reminders, of their responsibility to provide and maintain accurate WhoIs information and the ramifications of a failure to do so or respond to requests to do so, including termination of the Registration Agreement.

The measures to promote WhoIs accuracy described above strike a balance between the need to maintain the integrity of the WhoIs service, which facilitates the identification of those taking part in illegal or fraudulent behaviour, and the operating practices of the registry operator and Registrars, which aim to offer domain names to registrants in an efficient and timely manner. Awareness by registrants that we will actively take steps to maintain the accuracy of WhoIs information mitigates the potential for abuse in the TLD by discouraging abusive behaviour given that registrants may be identified, located and held liable for all actions in relation to their domain name."

---end of original reponse snippet on WHOIS Accuracy

We also acknowledge the work being undertaken by the Expert Working Group on gTLD Directory Services that will define future requirements for the delivery of WHOIS services. As this work will ultimately feed into a Board-initiated GNSO Policy Development Process (PDP) to serve as a foundation for the GNSO's creation of new consensus policies and requisite contract changes, this is the more appropriate mechanism for addressing the GAC Advice on this issue. Naturally, VoxPop will adopt the requirements which ensue from this important work with the understanding that such outcome will be enforced on successful new gTLD applicants through the Registry Agreement.

2. For Safeguards 2,4,5 and 6

With regard to the subsequent safeguards ("Safeguard 3. Security checks" will be dealt with separately below), our original response to Question 28 (Abuse Prevention and Mitigation) in our application, anticipated the GAC Communique.

We would point out that existing ICANN policy provides a more general and broader scope than requested by the GAC. As articulated in our original application, VoxPop, with the services of our registry services provider, ARI (AusRegistry International), has fully adopted the definition of abuse developed by the Registration Abuse Policies Working Group (Registration Abuse Policies Working Group Final Report 2010, at http://gnso.icann.org/issues/rap/rap-wg-final-report-29may10-en.pdf).

Under this policy, abusive behaviour in a TLD is defined as an action that:

– causes actual and substantial harm, or is a material predicate of such harm.
– is illegal or illegitimate, or is otherwise considered contrary to the intention and design of the mission⁄purpose of the TLD.

Our Abuse Prevention and Mitigation response included all the requisite elements requested by the GAC and more. We would encourage the Board to review our response in detail (Ref: Annex: Original Response to Question 28: Abuse Prevention and Mitigation).

3. Regarding Safeguard 3 Security Checks

On this one point, we do not believe the GAC request is within the scope of a Registry's responsibility and does not have a practical model for implementation. Registry Operators are not, and never have been charged with policing the Internet, nor should we be. Registry Operators do not have the expertise to carry out the requested "technical analysis". Indeed, only a handful of expert companies globally might have such expertise and the cost of employing such would be prohibitive. Imposing such a burden is beyond the bounds of the new gTLD application process.

4. Additional Safeguards Applicable to Category 1 Strings

The GAC Communique also included a list of 5 additional safeguards applicable to a list of names identified in Category 1. Our response to each of these safeguards is provided below.

i. GAC Safeguard Request: 1. Registry operators will include in their acceptable use policy that registrants comply with all applicable laws, including those that relate to privacy, data collection, consumer protection (including in relation to misleading and deceptive conduct), fair lending, debt collection, organic farming, disclosure of data, and financial disclosures.

As detailed in our response earlier to Abuse Prevention and Mitigation, VoxPop has clearly shown that we will not accept any kind of abusive behaviour particularly violation of all applicable laws. To inform registrants, VoxPop will publish a .SUCKS Anti Abuse Policy that will iterate all of the potential circumstances under which VoxPop may cancel or revoke a domain name registration. In addition, the VoxPop Registry Registrar Agreement (RRA) will require that Registrars ensure that (at the time of registration) the Registered Name Holder shall represent that, to the best of the Registered Name Holder's knowledge and belief, neither the registration of the Registered Name nor the manner in which it is directly or indirectly used infringes the legal rights of any third party and that the Registrant understands and accepts the .SUCKS Anti Abuse Policy defining acceptable use.

ii. GAC Safeguard Request 2: Registry operators will require registrars at the time of registration to notify registrants of this requirement.

As stated above, the VoxPop RRA will require that Registrars inform Registrants accordingly at the time of registration.

iii. GAC Safeguard Request 3: Registry operators will require that registrants who collect and maintain sensitive health and financial data implement reasonable and appropriate security measures commensurate with the offering of those services, as defined by applicable law and recognized industry standards.

VoxPop understands the GACs intention to ensure the security of personal health and financial data that may be collected by Registrants in the course of conducting their day-to-day business. However, it should be noted that the Registry has no ability to enforce the standards that the GAC is requesting nor should Registries have that scope of responsibility.

There are other industry examples of how it could be done.

Payment Card Industry (PCI) standards, which apply for the processing of credit card transactions for example, are administered and enforced by third parties with special expertise in this area. Audits on PCI compliance regularly take months to conduct.

VoxPop believes however that we can play a role in helping consumers understand under which circumstances they should consider providing sensitive health and financial data to a potential Registrant by issuing appropriate consumer data guidelines. VoxPop will include such guidelines on our website and provide references to same in our Terms and Conditions.

iv. GAC Safeguard Request 4: Establish a working relationship with the relevant regulatory, or industry self-regulatory, bodies, including developing a strategy to mitigate as much as possible the risks of fraudulent, and other illegal, activities.

Except for Cyber Bullying which is addressed below, VoxPop is not aware of any relevant regulatory, or industry self-regulatory, bodies that would be applicable to the .SUCKS platform. However, we acknowledge that both the RAA (Registrar Accreditation Agreement) and RA (Registry Agreement) have provisions for ensuring registrants shall not take any action inconsistent with the corresponding provisions of those Agreements or applicable law. Further, we will support and promote the Registrant’s Rights and Responsibilities Specification as required. Also under the RAA, Registrars will be required to establish and maintain a dedicated abuse contact point to respond to law enforcement, consumer protection, quasi-government or other similar authorities.

The RA also states that “Registry Operator shall take reasonable steps to investigate and respond to any reports from law enforcement and governmental and quasi-governmental agencies of illegal conduct in connection with the use of the TLD”, of course VoxPop will fully comply with this requirement. Clearly, the Board will also accept that complaint “handling” will be met by our referring such to the appropriate authorities or third party arbiters who have both the mandate and jurisdiction to conduct such mediation.

VoxPop suggests to the Board that this GAC Advice requirement is indeed addressed by specific clauses in both the RA and RAA as is necessary.

v. GAC Safeguard Request 5: Registrants must be required by the registry operators to notify to them a single point of contact which must be kept up-to-date, for the notification of complaints or reports of registration abuse, as well as the contact details of the relevant regulatory, or industry self-regulatory, bodies in their main place of business.

In our previous response on WHOIS VoxPop has indicated our commitment to implement the WHOIS ACCURACY PROGRAM SPECIFICATION as well as being committed to the requirement to adhere to the results of the current work being conducted by the Expert Working Group on gTLD Directory Services when it becomes a material part of the Registry Agreement

.

vi. GAC Supplemental Safeguard Request Applicable to .SUCKS: Applicants should develop clear policies and processes to minimise the risk of cyber bullying/harassment

VoxPop is pleased to point out that our application included relevant policies for the prevention of Cyber Bullying from the very start. In fact, ours is the ONLY application for .SUCKS to have done so. It is referenced in our original response to Question 18 and is further detailed in our response to Question 28 (see Annex below). Furthermore, even after GAC Early Warnings were issued referencing Cyber Bullying, competing .SUCKS applications continued to remain silent in their intent to establish policies against Cyber Bullying. VoxPop, on the other hand, submitted a PIC acknowledging that we will be held accountable under contract for our original policy commitments in this regard.

In short, if a complaint is made that any DotSUCKS site engages in cyber bullying (as defined by http://www.stopcyberbullying.org) and that complaint is proved, the site will be the subject of rapid takedown policies.

Generally, the takedown process will follow these steps:

- We will first suspend the domain name
- Investigate
- Refer the matter to an independent third party expert.

In this case we will engage industry subject matter experts to assist us in the development and implementation of the required policy and processes towards implementing our Cyber Bullying take down framework. Our plan is to create a framework similar to the UDRP process that would include assessment and review by a qualified unbiased third party of alleged Cyber Bullying claims. Finally, once the assessment is complete, we will then either restore or terminate the domain name as applicable. All of these provisions have been components of our application from the very start.

VoxPop is proud of our initial stance on Cyber Bullying and we believe that it is critical to the success of the DotSUCKS platform. More importantly, we believe that incorporating such policy in our original application reflects a commercial competitive advantage of our application. And, as the only application including such policy, we believe it is an integral component of the intellectual property which forms the basis of our platform.

We consider the GACs Advice on DotSUCKS generally to require that where and if such policy does not exist in an applicant’s submission, then the applicant(s) would be required to submit a formal application change request (none of the competing applications for DotSUCKS has provided provisions for Cyber Bullying). Such request must include proposed changes to the policies of their original submission to include the same (or similar) provision for Cyber Bullying which VoxPop already included in our original application. VoxPop further asserts that the ICANN Board must reject such change requests on the basis that they would be a material change to the policies of the operation of the registry, are clearly anti-competitive and would violate the intellectual property ownership contained in our original application which is now public.

The ICANN Board has the ability to reject specific applications based on non-adherence with GAC Advice. In this circumstance, the ICANN Board should clearly reject the other two applications for DotSUCKS (1-1279-43617 and 1-1596-35125) on the basis neither complies with GAC Advice to provide sufficient safeguards for Cyber Bullying. VoxPop has carefully reviewed both competitive applications as well as their filed PICs and can report that the term "Bullying" (let alone "Cyber Bullying") does not appear even once in either application. Allowing either of these applications to make such a change at this juncture is tantamount to allowing them to copy the intellectual property contained in VoxPop's original application. In so doing, such action removes a significant competitive advantage of our application and violates our intellectual property.

5. Further targeted safeguards for Category 1 Strings

The final section of the GAC Communique related to Category 1 strings apply only to a limited subset of the strings. VoxPop believes that .SUCKS is not one of the strings applicable to this requirement. It is not associated with market sectors which have clear and/or regulated entry requirements (such as: financial, gambling, professional services, environmental, health and fitness, corporate identifiers, and charity) in multiple jurisdictions. Therefore, we provide no detailed response to this section of the GAC Communique as none is required.

6. Additional Safeguards Applicable to Category 2 Strings

The GAC Communique has defined Category 2 strings as having "Restricted Registration Policies". This does not apply to the VoxPop application for .SUCKS which will be operated as an "open generic" gTLD. Therefore, we provide no detailed response to this section of the GAC Communique as none is required.

Annex

This is a recitation of our original response to question 28, Abuse Prevention and Mitigation. We have engaged ARI Registry Services (ARI) to deliver services for .SUCKS. ARI provides registry services for a number of TLDs including the .au ccTLD. For more background information on ARI please see the attachment 'Q28 – ARI Background & Roles.pdf'.

---start of original reponse to Q28

1 INTRODUCTION

The Registry will undertake a variety of steps to minimise abusive registrations and other activities in .SUCKS that have a negative impact on Internet users. We will utilise the ARI Anti-Abuse Service (AAS), which includes the implementation of the comprehensive .SUCKS Anti-

Abuse Policy (RAAP). This policy, developed in consultation with ARI, clearly defines abusive behaviour, identifies particular types of abusive behaviour, and specifies the steps to be taken in responding to such behaviour.

2 OVERVIEW

Owing to their extensive industry experience and established anti-abuse operations, ARI will implement and manage on our behalf various procedures and measures to prevent, detect, identify, and respond to abuse. ARI will automatically respond to information about the categories of abuse that fall within the scope of the ARI AAS, and forward to us all matters requiring determination by the registry operator and/or falling outside of the scope of ARI's AAS. This is described below in the context of the implementation of the .SUCKS Anti-Abuse Policy.

The ARI Anti-Abuse Service is structured to address the following categories of abuse:. Spam, Malware, Pornography, Fast Flux Hosting, Phishing, Illegal Access to other Computers or Networks, Pharming, Botnet command and control and Cyberbullying,   We nonetheless understand that it is our responsibility to minimise abusive registrations and other activities that have a negative impact on Internet users in the TLD. In recognition of this responsibility, we will play a hands-on role in the implementation of the ARI Anti-Abuse Service for .SUCKS. Our contract with ARI will contain SLA's to ensure that ARI's delivery of the Anti-Abuse Service is aligned with our strong commitment to minimise abuse in our TLD.

That strong commitment is further demonstrated by our adoption of many of the requirements proposed in the '2011 Proposed Security, Stability and Resiliency Requirements for Financial TLDs' (at http://www.icann.org/en/news/correspondence/aba-bits-to-beckstrom-crocker-20dec11-en.pdf) (the 'BITS Requirements). While these requirements were developed by the financial services sector to address potential abuses in financial TLDs, a number of the Requirements, if adapted and adopted in .SUCKS (which is not financial-related), will result in a more robust approach to combating abuse.

Consistent with Requirement 6 of the BITS Requirements, we will certify to ICANN on an annual basis our compliance with our Registry Agreement.

Please note that the various policies and practices that we have implemented to minimise abusive registrations and other activities that affect the rights of trademark holders are specifically described in our response to Question 29. Accordingly, they are NOT addressed in our response to this Question.

3 POLICY

In consultation with ARI we have developed a comprehensive Anti-Abuse Policy, which is the main instrument that captures our strategy in relation to abuse in the TLD.

3.1 Definition of Abuse

Abusive behaviour in a TLD may relate to the core domain name-related activities performed by Registrars and registries including, but not limited to:

– The allocation of registered domain names
– The maintenance of and access to registration information
– The transfer, deletion, and reallocation of domain names
– The manner in which the registrant uses the domain name upon creation

The scope of such activities makes it challenging to define abusive behaviour in a TLD. Defining abusive behaviour by reference to the stage in the domain name lifecycle in which the behaviour occurs also presents difficulty given that a particular type of abuse may occur at various stages of the life cycle.

With this in mind, ARI has fully adopted the definition of abuse developed by the Registration Abuse Policies Working Group (Registration Abuse Policies Working Group Final Report 2010, at http://gnso.icann.org/issues/rap/rap-wg-final-report-29may10-en.pdf), which does not focus on any particular stage in the domain name life cycle.

Under this policy, abusive behaviour in a TLD is defined as an action that:

– causes actual and substantial harm, or is a material predicate of such harm.

– is illegal or illegitimate, or is otherwise considered contrary to the intention and design of the mission/purpose of the TLD.

In applying this definition the following must be noted:

1. The party or parties harmed, and the severity and immediacy of the abuse, should be identified in relation to the specific alleged abuse.
2. The term "harm" is not intended to shield a party from fair market competition.
3. A predicate is a related action or enabler. There must be a clear link between the predicate and the abuse, and justification enough to address the abuse by addressing the predicate (enabling action).

For example, WhoIs data can be used in ways that cause harm to domain name registrants, intellectual property (IP) rights holders and Internet users. Harmful actions may include the generation of spam, the abuse of personal data, IP infringement, loss of reputation or identity theft, loss of data, phishing and other cybercrime-related exploits, harassment, stalking, or other activity with negative personal or economic consequences. Examples of predicates to these harmful actions are automated email harvesting, domain name registration by proxy/privacy services to aid wrongful activity, support of false or misleading registrant data, and the use of WhoIs data to develop large email lists for commercial purposes. The misuse of WhoIs data is therefore considered abusive because it is contrary to the intention and design of the stated legitimate purpose of WhoIs data.

3.2 Aims and Overview of Our Anti-Abuse Policy

The .SUCKS Anti-Abuse Policy will first ensure that registrants are on notice of the TLD policies, the ways in which the TLD will be monitored for abuse, the mechanisms for reporting abuse, and the manner in which we will respond to verified instances of abuse. We believe that unavoidable, “in your face” notification about these policies and procedures will serve as a deterrent to those seeking to register and use domain names for abusive purposes. The policy will be specifically called out in the registration process, easily accessible on the Abuse page of our registry website which will be linked directly from the home page, along with FAQs and contact information for reporting abuse.

Consistent with Requirements 15 and 16 of the BITS Requirements, our policy:

– Defines abusive behaviour in our TLD.

– Identifies types of actions that constitute abusive behaviour, consistent with our adoption of the RAPWG definition of ‘abuse’.

– Classifies abusive behaviours based on the severity and immediacy of the harm caused.

– Identifies how abusive behaviour can be notified to us and the steps that we will take to determine whether the notified behaviour is abusive.

– Identifies the actions that we may take in response to behaviour determined to be abusive.

Our RRA will oblige all Registrars to:
– comply with the .SUCKS Anti-Abuse Policy; and
– enter into a registration agreement with each registrant that obligates each registrant to comply with the Anti-Abuse Policy and each of the following requirements:
'operational standards, policies, procedures, and practices for the TLD established from time to time by the registry operator in a non-arbitrary manner and applicable to all Registrars, including affiliates of the registry operator, and consistent with ICANN's standards, policies, procedures, and practices and the registry operator's Registry Agreement with ICANN.' In addition, we will reserve the right to impose additional or revised registry operator operational standards, policies, procedures, and practices for the TLD which shall be effective upon thirty days notice by the registry operator to the Registrar. If there is a discrepancy between the terms required by this Agreement and the terms of the Registrar's registration agreement, the terms of this Agreement shall supersede those of the Registrar's registration agreement'.
Our RRA will additionally incorporate the following BITS Requirements:
– Requirement 7: Registrars must certify annually to ICANN and us compliance with ICANN's Registrar Accreditation Agreement (RAA) our Registry-Registrar Agreement (RRA).
– Requirement 9: Registrars must provide and maintain valid primary contact information (name, email address, and phone number) on their website.
– Requirement 14: Registrars must notify us immediately regarding any investigation or compliance action, including the nature of the investigation or compliance action by ICANN or any outside party (eg. law enforcement, etc.) along with the TLD impacted.

– Requirement 19: Registrars must disclose registration requirements on their website.
We will re-validate our RRAs at least annually, consistent with Requirement 10.

3.3 Anti-Abuse Policy
Our Anti-Abuse Policy is as follows:
Anti-Abuse Policy
Introduction:
The abusive registration and use of domain names in the TLD creates security and stability issues for all participants in the Internet environment and will not be tolerated.
Definition of Abusive Behaviour:
Abusive behaviour is an action that:
– causes actual and substantial harm, or is a material predicate of such harm; or
– is illegal or illegitimate, or is otherwise considered contrary to the intention and design of the mission/purpose of the TLD.
A 'predicate' is an action or enabler of harm.
'Material' means that something is consequential or significant.
Examples of abusive behaviour falling within this definition:
– 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 email in denial-of-service attacks.
– Phishing: the use of a fraudulently presented web site to deceive Internet users into divulging sensitive information such as usernames, passwords or financial data.

– Pharming: the redirecting of unknowing users to fraudulent web sites or services, typically through DNS hijacking or poisoning, in order to deceive Internet users into divulging sensitive information such as usernames, passwords or financial data.
– Wilful distribution of malware: the dissemination of software designed to infiltrate or cause damage to devices or to collect confidential data from users without their informed consent.
– Fast Flux hosting: the use of DNS to frequently change the location on the Internet to which the domain name of an Internet host or nameserver resolves in order 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 hosting may only be used with prior permission of the registry operator.
– Botnet command and control: the development and use of a command, agent, motor, service or software which is implemented: (1) to remotely control the computer or computer system of an Internet user without their knowledge or consent, (2) to generate direct denial of service (DDOS) attacks.
– Distribution of any form of pornography: the storage, publication, display and/or dissemination of pornographic
- Any form of cyber bullying defined as ‘any cyber-communication or publication posted or sent by a minor online, by instant message, e-mail, website, diary site, online profile, interactive game, handheld device, cellphone, game device, digital camera or video, webcam or use of any interactive device that is intended to frighten, embarrass, harass, hurt, set up, cause harm to, extort, or otherwise target another minor.’
– Illegal access to other computers or networks: the illegal accessing of computers, accounts, or networks belonging to another party, or attempt to penetrate security measures of another individual’s system (hacking). Also, any activity that might be used as a precursor to an attempted system penetration.

Detection of Abusive Behaviour:
Abusive behaviour in the TLD may be detected in the following ways:
– By us through our on-going monitoring activities and industry participation.
– By third parties (general public, law enforcement, government agencies, industry partners) through notification submitted to the abuse point of contact on our website, or industry alerts.
Reports of abusive behaviour will be notified immediately to the Registrar of record.
Intake and handling of reports of abusive behaviour:
The registry will maintain a web-based system (the “Abuse Reporting System” or the “ARS”) for reporting non-compliant registrations and/or registrants operating in a manner that violates .SUCKS Policies.
The ARS will facilitate prompt processing by queuing reports by category (e.g., phishing, pharming, spam, cyberbullying, etc.).
Personnel responsible for receiving and responding to abuse reports will be trained to recognize actions or activity that constitute abuse. Such personnel will have access to subject matter experts to assess reports about particular categories of abuse.

Handling of abusive behaviour:
Upon receipt of a report of abuse, a preliminary assessment will be performed in order to validate the report. Applying the definitions of types of abusive behaviours identified in this policy, we will classify each incidence of validated abuse into one of two categories based on the probable severity and immediacy of harm to registrants and Internet users. These categories are

provided below and are defined by reference to the action that may be taken by us. The examples of types of abusive behaviour falling within each category are illustrative only.
Category 1:
Probable Severity or Immediacy of Harm: Low
Examples of types of abusive behaviour: Spam, Malware, Pornography
Mitigation steps:
1. Investigate
2. Notify registrant (notice to cure)
Category 2:
Probable Severity or Immediacy of Harm: Medium to High
Examples of types of abusive behaviour: Fast Flux Hosting, Phishing, Illegal Access to other Computers or Networks, Pharming, Botnet command and control
Mitigation steps:
1. Suspend domain name
2. Investigate
3. Restore or terminate domain name
Category 3:
Probable Severity or Immediacy of Harm: Medium to High
Examples of types of abusive behaviour: Cyber bullying
Mitigation steps:
1. Suspend domain name
2. Investigate and refer to an independent third party expert. In this case we will engage industry subject matter experts to assist us in the development and implementation of the required policy and processes towards implementing our cyber bullying take down framework. Our plan is to create a framework similar to the UDRP process that would include assessment and review by a qualified unbiased third party of alleged Cyber Bullying claims.
3. Restore or terminate domain name
All reports of child abuse images will be automatically referred to the hotline designated to receive such reports.

Reports of illegal abusive behaviour submitted by a law enforcement agency, government or quasi-governmental agency will be reviewed and evaluated on an expedited basis, and the registry will comply with any specific instructions provided by the referring agency provided such steps are consistent with applicable law and respect any due process rights contained in applicable law. Please see section 4.3.2.2.1 below for information about the expedited process for qualifying agencies.

All reports of abusive behaviours will be date stamped and logged upon receipt. Subsequent processing, including suspension, referral, issuance of notice to cure, restore, termination, etc. will be logged.

The registry will conduct annual audits of reports of abusive behaviour, and adjust the operation of the .SUCKS registration policies and procedures, the ARS, and the .SUCKS policies on abusive behaviours as appropriate.
Note that these expected actions are intended to provide a guide to our response to abusive behaviour rather than any guarantee that a particular action will be taken.

The identification of abusive behaviour in the TLD, as defined above, shall give us the right, but not the obligation, to take such actions in accordance with the following text in the .SUCKS RRA, which provides that the registry operator:
‘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, or instruct Registrars to take such an action as we deem necessary in our discretion to;
1. protect the integrity and stability of the registry;
2.enforce TLD policies;
3. comply with any applicable laws, government rules or requirements, requests of law enforcement, or dispute resolution process;
4. avoid any liability, civil or criminal, on the part of the registry operator, as well as its affiliates, subsidiaries, officers, directors, and employees, per the terms of the registration agreement; and
5. correct mistakes made by the registry operator or any Registrar in connection with a domain name registration.
We reserve the right to place upon registry lock, hold or similar status a domain name during resolution of a dispute.
We also reserve the right to deny registration of a domain name to a registrant who has repeatedly engaged in abusive behaviour in our TLD or any other TLD.
Registrars only and not Resellers may offer proxy registration services to private individuals using the domain name for non-commercial purposes.
We may amend or otherwise modify this policy to keep abreast of changes in consensus policy or new and emerging types of abusive behaviour in the Internet.
Registrar’s failure to comply with this Anti-Abuse Policy shall constitute a material breach of the RRA, and shall give rise to the rights and remedies available to us under the RRA.

4 ABUSE PREVENTION AND MITIGATION

This section describes the implementation of our abuse related processes regarding:
– Building awareness of the Anti-Abuse Policy.
– Mitigating the potential for abusive behaviour.
– Identifying abusive behaviour.
– Handling abusive behaviour.

4.1. Awareness of Policy
The Anti-Abuse Policy will be published on the Abuse page of our registry website, which will be accessible and have clear links from the home page. In addition, the URL to the Abuse page will be included in all email correspondence to the registrant, thereby placing all registrants on notice of the applicability of the Anti-Abuse Policy to all domain names registered in our TLD. The Abuse page will, consistent with Requirement 8 of the BITS Requirements, provide registry contact information (name, email address, and phone number) to enable the public to communicate with us about TLD policies. The Abuse page will emphasise and evidence our commitment to combating abusive registrations by clearly identifying what our policy on abuse is and what effect our implementation of the policy may have on registrants. We anticipate that this clear message, which communicates our commitment to combating abusive registrations, will serve to minimise abusive registrations in our TLD.

4.2 Pre-emptive – Mitigating of the Potential for Abuse

The following practices and procedures will be adopted to mitigate the potential for abusive behaviour in our TLD.

4.2.1 ICANN Prescribed Measures
In accordance with our obligations as a registry operator, we will comply with all requirements in the 'gTLD Applicant Guidebook'. In particular, we will comply with the following measures prescribed by ICANN which serve to mitigate the potential for abuse in the TLD:
– DNSSEC deployment, which reduces the opportunity for pharming and other man-in-the-middle attacks. We will encourage Registrars and Internet Service Providers to deploy DNSSEC capable resolvers in addition to encouraging DNS hosting providers to deploy DNSSEC in an easy-to-use manner in order to facilitate deployment by registrants. DNSSEC deployment is further discussed in the context of our response to Question 43.
– Prohibition on Wild Carding as required by section 2.2 of Specification 6 of the Registry Agreement.
– Removal of Orphan Glue records (discussed below in '4.2.8 Orphan Glue Record Management').

4.2.2 Increasing Registrant Security Awareness
In accordance with our commitment to operating a secure and reliable TLD, we will attempt to improve registrant awareness of the threats of domain name hijacking, registrant impersonation and fraud, and emphasise the need for and responsibility of registrants to keep registration (including WhoIs) information accurate. Awareness will be raised by:
– Publishing the necessary information on the Abuse page of our registry website in the form of videos, presentations and FAQ's.
– Developing and providing to registrants and resellers Best Common Practices that describe appropriate use and assignment of domain auth Info codes and risks of misuse when the uniqueness property of this domain name password is not preserved.
The increase in awareness renders registrants less susceptible to attacks on their domain names owing to the adoption of the recommended best practices thus serving to mitigate the potential for abuse in the TLD. The clear responsibility on registrants to provide and maintain accurate registration information (including WhoIs) further serves to minimise the potential for abusive registrations in the TLD.

4.2.3 Mitigating the Potential for Abusive Registrations that Affect the Legal Rights of Others
Many of the examples of abusive behaviour identified in our Anti-Abuse Policy may affect the rights of trademark holders. While our Anti-Abuse Policy addresses abusive behaviour in a general sense, we have additionally developed specific policies and procedures to combat behaviours that affect the rights of trademark holders at start-up and on an ongoing basis. These include the implementation of a trademark claims service and a sunrise registration service at start-up and implementation of the UDRP, URS and PDDRP on an ongoing basis. The implementation of these policies and procedures serves to mitigate the potential for abuse in the TLD by ensuring that domain names are allocated to those who hold a corresponding trademark.
These policies and procedures are described in detail in our response to Question 29.

4.2.4 Safeguards Against Allowing for Unqualified Registrations
The eligibility restrictions for .SUCKS are outlined in our response to Question 18.

Eligibility restrictions will be implemented contractually through our RRA, which will require Registrars to include the following in their Registration Agreements:
– Registrant warrants that it satisfies eligibility requirements.
Where applicable, eligibility restrictions will be enforced through the adoption of the Charter Eligibility Dispute Resolution Policy or a similar policy, and Registrars will be obliged to require in their registration agreements that registrants agree to be bound by such policy and acknowledge that a registration may be cancelled in the event that a challenge against it under such policy is successful.
Providing an administrative process for enforcing eligibility criteria and taking action when notified of eligibility violations mitigates the potential for abuse. This is achieved through the risk of cancellation in the event that it is determined in a challenge procedure that eligibility criteria are not satisfied.

4.2.5 Registrant Disqualification
As specified in our Anti-Abuse Policy, we reserve the right to deny registration of a domain name to a registrant who has repeatedly engaged in abusive behaviour in our TLD or any other TLD.
Registrants, their agents or affiliates found through the application of our Anti-Abuse Policy to have repeatedly engaged in abusive registration will be disqualified from maintaining any registrations or making future registrations. This will be triggered when our records indicate that a registrant has had action taken against it an unusual number of times through the application of our Anti-Abuse Policy. Registrant disqualification provides an additional disincentive for qualified registrants to maintain abusive registrations in that it puts at risk even otherwise non-abusive registrations, through the possible loss of all registrations.
In addition, nameservers that are found to be associated only with fraudulent registrations will be added to a local blacklist and any existing or new registration that uses such fraudulent NS record will be investigated.
The disqualification of ‘bad actors’ and the creation of blacklists mitigates the potential for abuse by preventing individuals known to partake in such behaviour from registering domain names.

4.2.6 Restrictions on Proxy Registration Services
Whilst it is understood that implementing measures to promote WhoIs accuracy is necessary to ensure that the registrant may be tracked down, it is recognised that some registrants may wish to utilise a proxy registration service to protect their privacy. In the event that Registrars elect to offer such services, the following conditions apply:
– Proxy registration services may only be offered by Accredited Registrars and NOT resellers.
– Registrars must obtain and maintain the actual WhoIs data from the registrant.
– Registrars must provide Law Enforcement Agencies (LEA) with the actual WhoIs data upon receipt of a verified request.
– Proxy registration services may only be made available to private individuals using the domain name for non-commercial purposes.
These conditions will be implemented contractually by inclusion of corresponding clauses in the RRA as well as being published on the Abuse page of our registry website. Individuals and organisations will be encouraged through our Abuse page to report any domain names they believe violate the above restrictions, following which appropriate action may be taken by us.
Publication of these conditions on the Abuse page of our registry website ensures that registrants are aware that despite utilisation of a proxy registration service, actual WhoIs

information will be provided to LEA upon request in order to hold registrants liable for all actions in relation to their domain name. The certainty that WhoIs information relating to domain names which draw the attention of LEA will be disclosed results in the TLD being less attractive to those seeking to register domain names for abusive purposes, thus mitigating the potential for abuse in the TLD.

4.2.7 Registry Lock
Certain mission-critical domain names such as transactional sites, email systems and site supporting applications may warrant a higher level of security. Whilst we will take efforts to promote the awareness of security amongst registrants, it is recognised that an added level of security may be provided to registrants by 'registry locking' the domain name thereby prohibiting any updates at the registry operator level. The registry lock service will be offered to all Registrars who may request this service on behalf of their registrants in order to prevent unintentional transfer, modification or deletion of the domain name. This service mitigates the potential for abuse by prohibiting any unauthorised updates that may be associated with fraudulent behaviour. For example, an attacker may update nameservers of a mission-critical domain name, thereby redirecting customers to an illegitimate website without actually transferring control of the domain name.
Upon receipt of a list of domain names to be placed on registry lock by an authorised representative from a Registrar, ARI will:
1. Validate that the Registrar is the Registrar of record for the domain names.
2. Set or modify the status codes for the names submitted to serverUpdateProhibited, serverDeleteProhibited and/or serverTransferProhibited depending on the request.
3. Record the status of the domain name in the Shared Registration System (SRS).
4. Provide a monthly report to Registrars indicating the names for which the registry lock service was provided in the previous month.

4.2.8 Orphan Glue Record Management
The ARI registry SRS database does not allow orphan records. Glue records are removed when the delegation point NS record is removed. Other domains that need the glue record for correct DNS operation may become unreachable or less reachable depending on their overall DNS service architecture. It is the registrant's responsibility to ensure that their domain name does not rely on a glue record that has been removed and that it is delegated to a valid nameserver. The removal of glue records upon removal of the delegation point NS record mitigates the potential for use of orphan glue records in an abusive manner.

4.2.9 Promoting WhoIs Accuracy
Inaccurate WhoIs information significantly hampers the ability to enforce policies in relation to abuse in the TLD by allowing the registrant to remain anonymous. In addition, LEAs rely on the integrity and accuracy of WhoIs information in their investigative processes to identify and locate wrongdoers. In recognition of this, we will implement a range of measures to promote the accuracy of WhoIs information in our TLD including:
– Random monthly audits: registrants of randomly selected domain names are contacted by telephone using the provided WhoIs information by a member of the ARI Abuse and Compliance Team in order to verify all WhoIs information. Where the registrant is not contactable by telephone, alternative contact details (email, postal address) will be used to contact the registrant, who must then provide a contact number that is verified by the member of the ARI Policy Compliance team. In the event that the registrant is not able to be contacted by any of

the methods provided in WhoIs, the domain name will be cancelled following five contact attempts or one month after the initial contact attempt (based on the premise that a failure to respond is indicative of inaccurate WhoIs information and is grounds for terminating the registration agreement).

– Semi-annual audits: to identify incomplete WhoIs information. Registrants will be contacted using provided WhoIs information and requested to provide missing information. In the event that the registrant fails to provide missing information as requested, the domain name will be cancelled following five contact attempts or one month after the initial contact attempt.

– Email reminders: to update WhoIs information to be sent to registrants every 6 months.

– Reporting system: a web-based submission service for reporting WhoIs accuracy issues available on the Abuse page of our registry website.

– Analysis of registry data: to identify patterns and correlations indicative of inaccurate WhoIs (eg repetitive use of fraudulent details).

Registrants will continually be made aware, through the registry website and email reminders, of their responsibility to provide and maintain accurate WhoIs information and the ramifications of a failure to do so or respond to requests to do so, including termination of the Registration Agreement.

The measures to promote WhoIs accuracy described above strike a balance between the need to maintain the integrity of the WhoIs service, which facilitates the identification of those taking part in illegal or fraudulent behaviour, and the operating practices of the registry operator and Registrars, which aim to offer domain names to registrants in an efficient and timely manner. Awareness by registrants that we will actively take steps to maintain the accuracy of WhoIs information mitigates the potential for abuse in the TLD by discouraging abusive behaviour given that registrants may be identified, located and held liable for all actions in relation to their domain name.

4.3 Reactive – Identification

The methods by which abusive behaviour in our TLD may be identified are described below. These include detection by ARI and notification from third parties. These methods serve to merely identify and not determine whether abuse actually exists. Upon identification of abuse, the behaviour will be handled in accordance with '4.4 Abuse Handling'.

Any abusive behaviour identified through one of the methods below will, in accordance with Requirement 13 of the BITS Requirements, be notified immediately to relevant Registrars.

4.3.1 Detection – Analysis of Data

ARI will routinely analyse registry data in order to identify abusive domain names by searching for behaviours typically indicative of abuse. The following are examples of the data variables that will serve as indicators of a suspicious domain name and may trigger further action by the ARI Abuse and Compliance Team:

– Unusual Domain Name Registration Practices: practices such as registering hundreds of domains at a time, registering domains which are unusually long or complex or include an obvious series of numbers tied to a random word (abuse40, abuse50, abuse60) may, when considered as a whole, be indicative of abuse.

– Domains or IP addresses identified as members of a Fast Flux Service Network (FFSN): ARI uses the formula developed by the University of Mannheim and tested by participants of the Fast Flux PDP WG to determine members of this list. IP addresses appearing within identified FFSN domains, as either NS or A records shall be added to this list.

– An Unusual Number of Changes to the NS record: the use of fast-flux techniques to disguise the location of web sites or other Internet services, to avoid detection and mitigation efforts, or to host illegal activities is considered abusive in the TLD. Fast flux techniques use DNS to frequently change the location on the Internet to which the domain name of an Internet host or nameserver resolves. As such an unusual number of changes to the NS record may be indicative of the use of fast-flux techniques given that there is little, if any, legitimate need to change the NS record for a domain name more than a few times a month.
– Results of WhoIs audits: The audits conducted to promote WhoIs accuracy described above are not limited to serving that purpose but may also be used to identify abusive behaviour given the strong correlation between inaccurate WhoIs data and abuse.
– Analysis of cross-validation of registrant WhoIs data against WhoIs data known to be fraudulent.
– Analysis of Domain Names belonging to a registrant subject to action under the Anti-Abuse Policy: in cases where action is taken against a registrant through the application of the Anti-Abuse Policy, we will also investigate other domain names by the same registrant (same name, nameserver IP address, email address, postal address etc).

4.3.2 Abuse Reported by Third Parties
Whilst we are confident in our abilities to detect abusive behaviour in the TLD owing to our robust ongoing monitoring activities, we recognise the value of notification from third parties to identify abuse. To this end, we will incorporate notifications from the following third parties in our efforts to identify abusive behaviour:
– Industry partners through ARI's participation in industry forums which facilitate the sharing of information.
– LEA through a single abuse point of contact (our Abuse page on the registry website, as discussed in detail below) and an expedited process (described in detail in '4.4 Abuse Handling') specifically for LEA.
– Members of the general public through a single abuse point of contact (our Abuse page on the registry website).

4.3.2.1 Industry Participation and Information Sharing
ARI is a member of the Registry Internet Safety Group (RISG), whose mission is to facilitate data exchange and promulgate best practices to address Internet identity theft, especially phishing and malware distribution. In addition, ARI coordinates with the Anti-Phishing Working Group (APWG) and other DNS abuse organisations and is subscribed to the NXdomain mailing list. ARI's strong participation in the industry facilitates collaboration with relevant organisations on abuse-related issues and ensures that ARI is responsive to new and emerging domain name abuses.
The information shared as a result of this industry participation will be used to identify domain names registered or used for abusive purposes. Information shared may include a list of registrants known to partake in abusive behaviour in other TLDs. Whilst presence on such lists will not constitute grounds for registrant disqualification, ARI will investigate domain names registered to those listed registrants and take action in accordance with the Anti-Abuse Policy. In addition, information shared regarding practices indicative of abuse will facilitate detection of abuse by our own monitoring activities.

4.3.2.2 Single Abuse Point of Contact on Website

In accordance with section 4.1 of Specification 6 of the Registry Agreement, we will establish a single abuse point of contact (SAPOC) responsible for addressing and providing a timely response to abuse complaints concerning all names registered in the TLD through all Registrars of record, including those involving a reseller. Complaints may be received from members of the general public, other registries, Registrars, LEA, government and quasi-governmental agencies and recognised members of the anti-abuse community.

The SAPOC's accurate contact details (email and mailing address as well as a primary contact for handling inquiries related to abuse in the TLD) will be provided to ICANN and published on the Abuse page of our registry website, which will also include:

– All public facing policies in relation to the TLD, including the Anti-Abuse Policy.

– A web-based submission service for reporting inaccuracies in WhoIs information.

– Registrant Best Practices.

– Conditions that apply to proxy registration services and direction to the SAPOC to report domain names that violate the conditions.

As such, the SAPOC may receive complaints regarding a range of matters including but not limited to:

– Violations of the Anti-Abuse Policy.

– Inaccurate WhoIs information.

– Violation of the restriction of proxy registration services to individuals.

The SAPOC will be the primary method by which we will receive notification of abusive behaviour from third parties. It must be emphasised that the SAPOC will be the initial point of contact following which other processes will be triggered depending on the identity of the reporting organisation. Accordingly, separate processes for identifying abuse exist for reports by LEA/government and quasi-governmental agencies and members of the general public. These processes will be described in turn below.

4.3.2.2.1 Notification by LEA of Abuse

We recognise that LEA, governmental and quasi-governmental agencies may be privy to information beyond the reach of others which may prove critical in the identification of abusive behaviour in our TLD. As such, we will provide an expedited process which serves as a channel of communication for LEA, government and quasi-governmental agencies to, amongst other things, report illegal conduct in connection with the use of the TLD.

The process will involve prioritisation and prompt investigation of reports identifying abuse from those organisations. The steps in the expedited process are summarised as follows:

1. ARI's Abuse and Compliance Team will publish a mechanism for verifying relevant LEA, government and quasi-governmental agencies eligible to use the expedited process, depending on the mission/purpose and jurisdiction of our TLD. In addition, the Team will pro-actively identify and reach-out to relevant agencies.

2. We will publish contact details on the Abuse page of the registry website for the SAPOC to be utilised by only those taking part in the expedited process.

3. All calls to this number will be responded to by the ARI Service Desk on a 24/7 basis. All calls will result in the generation of a ticket in ARI's case management system (CMS).

4. The identity of the reporting agency will be identified using the established means of verification (ARI's Security Policy has strict guidelines regarding the verification of external parties over the telephone). If no means of verification has been established, the report will be immediately escalated to the ARI Abuse and Compliance Team. Results of verification will be recorded against the relevant CMS ticket.

6. Upon verification of the reporting agency, the ARI Service Desk will obtain the details necessary to adequately investigate the report of abusive behaviour in the TLD. This information will be recorded against the relevant CMS ticket.
7. Reports from verified agencies may be provided in the Incident Object Description Exchange Format (IODEF) as defined in RFC 5070. Provision of information in the IODEF will improve our ability to resolve complaints by simplifying collaboration and data sharing.
8. Tickets will then be forwarded to the ARI Abuse and Compliance Team to be dealt with in accordance with '4.4 Abuse Handling'.

4.3.2.2.2 Notification by General Public of Abuse

Abusive behaviour in the TLD may also be identified by members of the general public including but not limited to other registries, Registrars or security researchers. The steps in this notification process are summarised as follows:
1. We will publish contact details on the Abuse page of the registry website for the SAPOC (note that these contact details are not the same as those provided for the expedited process).
2. All calls to this number will be responded to by the ARI Service Desk on a 24/7 basis. All calls will result in the generation of a CMS ticket.
3. The details of the report identifying abuse will be documented in the CMS ticket using a standard information gathering template.
4. Tickets will be forwarded to the ARI Abuse and Compliance Team, to be dealt with in accordance with '4.4 Abuse Handling'.

All reports of child abuse images will be automatically referred to the hotline designated to receive such reports.

4.4 Abuse Handling

Upon being made aware of abuse in the TLD, whether by ongoing monitoring activities or notification from third parties, the ARI Abuse and Compliance Team will perform the following functions:

4.4.1 Preliminary Assessment and Categorisation

Each report of purported abuse will undergo an initial preliminary assessment by the ARI Abuse and Compliance Team to determine the legitimacy of the report. This step may involve simply visiting the offending website and is intended to weed out spurious reports, and will not involve the in-depth investigation needed to make a determination as to whether the reported behaviour is abusive.

Where the report is assessed as being legitimate, the type of activity reported will be classified as one of the types of abusive behaviour as found in the Anti-Abuse Policy by the application of the definitions provided. In order to make this classification, the ARI Abuse and Compliance Team must establish a clear link between the activity reported and the alleged type of abusive behaviour such that addressing the reported activity will address the abusive behaviour.

While we recognise that each incident of abuse represents a unique security threat and should be mitigated accordingly, we also recognise that prompt action justified by objective criteria are key to ensuring that mitigation efforts are effective. With this in mind, we have categorised the actions that we may take in response to various types of abuse by reference to the severity and immediacy of harm. This categorisation will be applied to each validated report of abuse and actions will be taken in accordance with the table below. It must be emphasised that the actions to mitigate the identified type of abuse in the table are merely intended to provide a rough guideline and may vary upon further investigation.

Category 1
Probable Severity or Immediacy of Harm: Low
Examples of types of abusive behaviour: Spam, Malware
Mitigation steps:
1. Investigate
2. Notify registrant
Category 2
Probable Severity or Immediacy of Harm: Medium to High
Examples of types of abusive behaviour: Fast Flux Hosting, Phishing, Illegal Access to other Computers or Networks, Pharming, Botnet command and control
Mitigation steps:
1. Suspend domain name
2. Investigate
3. Restore or terminate domain name
The mitigation steps for each category will now be described:
Category 3:
Probable Severity or Immediacy of Harm: Medium to High
Examples of types of abusive behaviour: Cyber bullying
Mitigation steps:
1. Suspend domain name
2. Investigate by an independent third party. In this case we will engage industry subject matter experts to assist us in the development and implementation of the required policy and processes towards implementing our cyber bullying take down framework. Our plan is to create a framework similar to the UDRP process that would include assessment and review by a qualified unbiased third party of alleged Cyber Bullying claims.

4.4.2 Investigation – Category 1
Types of abusive behaviour that fall into this category include those that represent a low severity or immediacy of harm to registrants and Internet users. These generally include behaviours that result in the dissemination of unsolicited information or the publication of illegitimate information. While undesirable, these activities do not generally present such an immediate threat as to justify suspension of the domain name in question. We will contact the registrant to instruct that the breach of the Anti-Abuse Policy be rectified. If the ARI Abuse and Compliance Team's investigation reveals that the severity or immediacy of harm is greater than originally anticipated, the abusive behaviour will be escalated to Category 2 and mitigated in accordance with the applicable steps. These are described below. The assessment made and actions taken will be recorded against the relevant CMS ticket.

4.4.3 Suspension – Category 2
Types of abusive behaviour that fall into this category include those that represent a medium to high severity or immediacy of harm to registrants and Internet users. These generally include behaviours that result in intrusion into other computers' networks and systems or financial gain by fraudulent means. Following notification of the existence of such behaviours, the ARI Abuse and Compliance Team will suspend the domain name pending further investigation to determine whether the domain name should be restored or cancelled. Cancellation will result if, upon further investigation, the behaviour is determined to be one of the types of abuse defined in the Anti-Abuse Policy. Restoration of the domain name will result where further investigation determines that abusive behaviour, as defined by the Anti-Abuse Policy, does not exist. Due to

the higher severity or immediacy of harm attributed to types of abusive behaviour in this category, ARI will, in accordance with their contractual commitment to us in the form of SLA's, carry out the mitigation response within 24 hours by either restoring or cancelling the domain name. The assessment made and actions taken will be recorded against the relevant CMS ticket.

Phishing is considered to be a serious violation of the Anti-Abuse Policy owing to its fraudulent exploitation of consumer vulnerabilities for the purposes of financial gain. Given the direct relationship between phishing uptime and extent of harm caused, we recognise the urgency required to execute processes that handle phish domain termination in a timely and cost effective manner. Accordingly, the ARI Abuse and Compliance Team will prioritise all reports of phishing from brand owners, anti-phishing providers or otherwise and carry out the appropriate mitigation response within 12 hours in accordance with the SLA's in place between us and ARI. In addition, since a majority of phish domains are subdomains, we believe it is necessary to ensure that subdomains do not represent an unregulated domain space to which phishers are known to gravitate. Regulation of the subdomain space is achieved by holding the registrant of the parent domain liable for any actions that may occur in relation to subdomains. In reality, this means that where a subdomain determined to be used for phishing is identified, the parent domain may be suspended and possibly cancelled, thus effectively neutralising every subdomain hosted on the parent. In our RRA we will require that Registrars ensure that their Registration Agreements reflect our ability to address phish subdomains in this manner.

4.4.3 Suspension – Category 3
Types of abusive behaviour that fall into this category are anything defined as cyber bullying per http://www.stopcyberbullying.org. This organization represents one example of an organization that could be engaged to formulate the .SUCKS TLD's cyber bullying policies. Notification of the alleged existence of cyberbullying shall be reviewed within 8 business hours of receipt and promptly investigated to rule out any abusive reports. After ruling out clearly abusive reports, the ARI Abuse and Compliance Team will suspend the domain name pending further investigation to determine whether the domain name should be restored or cancelled. As this represents a very specialized form of abuse, ARI will pass all complaints of cyberbullying (including reports deemed to have been abusive) on to our partner (yet to be determined), whose organization will conduct the investigation under contract. Cancellation will result if, as a result of the investigation, the behaviour is determined to be one of the types of abuse defined in the Anti-Abuse Policy. Restoration of the domain name will result where further investigation determines that abusive behaviour, as defined by the Anti-Abuse Policy, does not exist. Due to the higher severity or immediacy of harm attributed to types of abusive behaviour in this category, ARI will, in accordance with their contractual commitment to us in the form of SLA's, carry out the mitigation response within 24 hours by either restoring or cancelling the domain name. The assessment made and actions taken will be recorded against the relevant CMS ticket.

4.4.5 Executing LEA Instructions
We understand the importance of our role as a registry operator in addressing consumer vulnerabilities and are cognisant of our obligations to assist LEAs, government and quasi-governmental agencies in the execution of their responsibilities. As such, we will make all reasonable efforts to ensure the integration of these agencies into our processes for the identification and handling of abuse by, amongst other things:
1. Providing expedited channels of communication (discussed above).

2. Notifying LEA of abusive behaviour believed to constitute evidence of a commission of a crime eg distribution of child pornography.
3. Sharing all available information upon request from LEA utilising the expedited process, including results of our investigation.
4. Providing bulk WhoIs information upon request from LEA utilising the expedited process.
5. Acting on instructions from a verified reporting agency.
It is anticipated that these actions will assist agencies in the prevention, detection, investigation, prosecution or punishment of criminal offences or breaches of laws imposing penalties. The relevant agencies are not limited to those enforcing criminal matters but may also include those enforcing civil matters in order to eliminate consumer vulnerabilities.
Upon notification of abusive behaviour by LEA, government or quasi– governmental agencies through the expedited process and verification of the reporting agency, a matter will be immediately communicated to us for our consideration. If we do not instruct ARI to refer the matter to us for our resolution, the CMS ticket will be forwarded to the ARI Abuse and Compliance Team, which will take one of the following actions:
1. The reported behaviour will be subject to preliminary assessment and categorisation as described above. The reported behaviour will then be mitigated based on the results of the categorisation. A report describing the manner in which the notification from the agency was handled will be provided to the agency within 24 hours. This report will be recorded against the relevant CMS ticket.
OR
2. Where specific instructions are received from the reporting agency in the required format, ARI will act in accordance with those instructions provided that they do not result in the contravention of applicable law. ARI will, in accordance with their contractual commitment to us in the form of SLA’s, execute such instructions within 12 hours. The following criteria must be satisfied by the reporting agency at this stage:
a. The request must be made in writing to ARI using a Pro Forma document on the agency’s letterhead. The Pro Forma document will be sent to the verified agency upon request.
b. The Pro Forma document must be delivered to ARI by fax.
c. The Pro Forma document must:
i. Describe in sufficient detail the actions the agency seeks ARI to take.
ii. Provide the domain name/s affected.
iii. Certify that the agency is an ‘enforcement body’ for the purposes of the Privacy Act 1988 (Cth) or local equivalent.
iv. Certify that the requested actions are required for the investigation and/or enforcement of relevant legislation which must be specified.
v. Certify that the requested actions are necessary for the agency to effectively carry out its functions.
Following prompt execution of the request, a report will be provided to the agency in a timely manner. This report will be recorded against the relevant CMS ticket.
Finally, whilst we do not anticipate the occurrence of a security situation owing to our robust systems and processes deployed to combat abuse, we are aware of the availability of the Expedited Registry Security Request Process to inform ICANN of a present or imminent security situation and to request a contractual waiver for actions we might take or have taken to mitigate or eliminate the security concern.

5 RESOURCES

This function will be performed by ARI. Abuse services are supported by the following departments:

– Abuse and Compliance Team (6 staff)
– Development Team (11 staff)
– Service Desk (14 staff)

A detailed list of the departments, roles and responsibilities in ARI is provided as attachment 'Q28 – ARI Background & Roles.pdf'. This attachment describes the functions of the above teams and the exact number and nature of staff within.
The number of resources required to design, build, operate and support the SRS does not vary significantly with, and is not linearly proportional to, the number or size of TLDs that ARI provides registry services to.
ARI provides registry backend services to 5 TLDs and has a wealth of experience in estimating the number of resources required to support a registry system.
Based on past experience ARI estimates that the existing staff is adequate to support a registry system that supports in excess of 50M domains. Since .SUCKS projects 10,049 domains, 0.0205% of these resources are allocated to .SUCKS. See attachment 'Q28 – Registry Scale Estimates & Resource Allocation.xlsx' for more information.
ARI protects against loss of critical staff by employing multiple people in each role. Staff members have a primary role plus a secondary role for protection against personnel absence. Additionally ARI can scale resources as required.

ARI's Anti-Abuse Service serves to prevent and mitigate abusive behaviour in the TLD as well as activities that may infringe trademarks. These responsibilities will be undertaken by three teams. ARI's Development Team will be responsible for developing the technical platforms and meeting technical requirements needed to implement the procedures and measures adopted to mitigate the potential for abuse, identify abuse and handle identified abuse. ARI's Abuse and Compliance Team will be responsible for the ongoing implementation of measures to minimise abusive registrations and other activities that have a negative impact on Internet users. ARI's Service Desk will be responsible for responding to reports of abuse received through the abuse point of contact on the registry's website and logging these in a ticket in ARI's case management system.
The responsibilities of these teams relevant to the initial implementation and ongoing maintenance of our measures to minimise abusive registrations and other activities that affect the rights of trademark holders are described in our response to Question 29.
All of the responsibilities undertaken by ARI's Development Team, Abuse and Compliance Team, and Service Desk are inclusive in ARI's Managed TLD Registry services fee, which is accounted for as an outsourcing cost in our response to Question 47. The resources needs of these teams have been determined by applying the conservative growth projections for our TLD (which are identified in our response to Question 48) to the team's responsibilities at start-up and on an ongoing basis.

5.1 ARI Development Team
All tools and systems needed to support the initial and ongoing implementation of measures adopted to mitigate the potential for abuse, identify abuse and handle identified abuse will be developed and maintained by ARI. ARI has a software development department dedicated to

this purpose which will ensure that the tools are fit for purpose and adjusted as requirements change.

ARI’s Development Team participate actively in the industry; this facilitates collaboration with relevant organisations on abuse related issues and ensures that the ARI Development Team is responsive to new and emerging domain name abuses and the tools and systems required to be built to address these abuses. This team consists of:

– 1 Development Manager
– 2 Business Analysts
– 6 Developers
– 2 Quality Analysts

5.2 ARI Abuse and Compliance Team

ARI’s Abuse and Compliance Team will be staffed by six full-time equivalent positions. These roles will entail the following:

Policy Compliance Officers: A principal responsibility of the Policy Compliance Officers will be handling notifications of abuse through the SAPOC. This will involve managing the expedited process, identifying and categorising suspected abuse according to our Anti-Abuse Policy, and carrying out the appropriate mitigation response for all categorised abuses. When abuse is identified, Policy Compliance Officers will investigate other domain names held by a registrant whose domain name is subject to a mitigation response. They will maintain a list of and disqualify registrants found to have repeatedly engaged in abusive behaviour. They will also be responsible for analysing registry data in search of behaviours indicative of abuse, reviewing industry lists in search of data that may identify abuse in the TLD.

Another key responsibility of Policy Compliance Officers will be implementing measures to promote WhoIs accuracy (including managing and addressing all reports of inaccurate WhoIs information received from the web submission service) and verifying the physical address provided by a registrant against various databases for format and content requirements for the region.

Policy Compliance Officers will act on the instructions of verified LEA and Dispute Resolution Providers and participate in ICANN and industry groups involved in the promulgation of policies and best practices to address abusive behaviour. They will escalate complaints and issues to the Legal Manager when necessary and communicate with all relevant stakeholders (Registrars, registrants, LEA, general public) as needed in fulfilling these responsibilities. This role will be provided on a 24/7 basis, supported outside of ordinary business hours by ARI’s Service Desk.

Policy Compliance Officers will be required to have the following skills/qualifications: customer service/fault handling experience, comprehensive knowledge of abusive behaviour in a TLD and related policies, Internet industry knowledge, relevant post-secondary qualification, excellent communication and professional skills, accurate data entry skills, high-level problem solving skills, and high-level computer skills.

Legal Manager: The Legal Manager will be responsible for handling all potential disputes arising in connection with the implementation of ARI’s Anti-Abuse service and related policies. This will involve assessing escalated complaints and issues, liaising with Legal Counsel and the registry operator, resolving disputes and communicating with all relevant stakeholders (Registrars, registrants, LEA, general public) as needed in fulfilling these responsibilities. The Legal Manager will be responsible for forwarding all matters requiring determination by the registry operator which fall outside the scope of ARI’s Anti-Abuse functions. The Legal Manager will be required to have the following skills/qualifications: legal background (in particular, intellectual property/information technology law) or experience with relevant tertiary or post-graduate qualifications, dispute resolution experience, Internet industry experience, strong negotiation skills, excellent communication and professional skills, good computer skills, high-level problem solving skills.

Legal Counsel: A qualified lawyer who will be responsible for all in-house legal advice, including responding to LEA and dealing with abusive behaviour.

The team consists of:

– 4 Policy Compliance Officers
– 1 Legal Manager
– 1 Legal Counsel

5.3 ARI Service Desk

ARI’s Service Desk will be staffed by 14 full-time equivalent positions. Responsibilities of Service Desk relevant to ARI’s Anti-Abuse Service include the following: responding to notifications of abuse through the abuse point of contact and expedited process for LEA, logging notifications as a ticket in ARI’s case management system, notifying us of a report received through the expedited process for LEA, government and quasi-governmental agencies, and forwarding tickets to ARI’s Abuse and Compliance team for resolution in accordance with the Anti-Abuse Policy.

For more information on the skills and esponsibilities of these roles please see the in-depth resources section in response to Question 31.

Based on the projections and the experience of ARI, the resources described here are more than sufficient to accommodate the needs of .SUCKS.

The use of these resources and the services they enable is included in the fees paid to ARI which are described in the financial responses.

---end of original reponse to Q28