Exhibit 1

Code of Conduct Exemption Request Form

Internet Corporation for Assigned Names and Numbers ("ICANN")
12025 Waterfront Drive, Suite 300
Los Angeles, California 90094
Attention: New gTLD Program Staff

RE: Request for Exemption from Registry Operator Code of Conduct

Translations, ("Registry Operator"), in connection with the execution of the Registry
Agreement for the .TRANSLATIONS TLD (the "Registry Agreement"), hereby requests an
exemption from the obligations of the Registry Operator Code of Conduct set forth in
Specification 9 to the Registry Agreement (the "Code of Conduct"). Pursuant to such request,
Registry Operator confirms that each of the following statements is true and correct
(collectively, referred to as the "Statements"):

1. All domain name registrations in the TLD are registered to, and maintained by, Registry
Operator for the exclusive use of Registry Operator or its Affiliate (as defined in the Registry
Agreement);

2. Registry Operator does not sell, distribute or transfer control or use of any registrations in
the TLD to any third party that is not an Affiliate of Registry Operator; and

3. Application of the Code of Conduct to the TLD is not necessary to protect the public
interest for the following reasons:

The operation of the .TRANSLATIONS TLD will allow the Registry Operator to reflect and
operate its key and most distinctive brand. The public interest will benefit from the fact that
the Registry Operator is able to do so in a controlled way. This control by the Registry
Operator can be guaranteed more easily when the Code of Conduct does not apply to the
operation of the .TRANSLATIONS TLD. Hence the public interest will benefit from the
exemption of the Code of Conduct and the Registry Operator can think of no reason why the
application of the Code of Conduct to the TLD would be necessary to protect the public
interest.

Registry Operator represents that the registration policies attached hereto as Schedule A are a
true and correct copy of the Registry Operator's registration policies for the TLD.

Registry Operator agrees to notify ICANN promptly in writing in the event any of the
Statements has become untrue (whether before or after an exemption has been granted).

Registry Operator further acknowledges and agrees that the Exemption will be void if at any
time any of the Statements has become untrue.

Submitted by: [Redacted]
Position: CEO
Date Noted: November 5th, 2013
Email: [Redacted]

.TRANSLATIONS DOMAIN REGISTRATION AND USE POLICY

1 INTRODUCTION

Translations company intends to request an exemption from clause 1b of the Registry Operator Code of Conduct (Specification 9) pursuant to clause 6 of the Code of Conduct to enable it to register domain names in its own right in this TLD. Registrations will not be made commercially available; all domain name registrations in the TLD will be registered to and maintained by Translations in its capacity as Registry Operator, for its own exclusive use. It will not sell, distribute or transfer control or use of any registration in the TLD to any third party that is not its Affiliate.

For clarification and to reflect the unique roles of the stakeholders in the .translations TLD, the following terms, where used in this document, have the following meaning:

"Registry operator" means the entity submitting an application to ICANN for the operation and management of a TLD. All references to "us", "we" or "our" are to be taken as references to the Registry operator.

"Affiliate" means, as defined in Clause 2.9(c) of the Registry Agreement, "a person or entity that, directly or indirectly, through one or more intermediaries, controls, is controlled by, or is under common control with, the person or entity specified, and (ii) 'control' (including the terms 'controlled by' and 'under common control with') means the possession, directly or indirectly, of the power to direct or cause the direction of the management or policies of a person or entity, whether through the ownership of securities, as trustee or executor, by serving as an employee or a member of a board of directors or equivalent governing body, by contract, by credit arrangement or otherwise."

"Registrant" means the registered holder of a domain name, in this case the Registry operator, consistent with the eligibility restrictions in our TLD as described in our response to Question 18 of our Application No.1-850-14889.

Our comprehensive Acceptable Registration and Use Policy, developed in consultation with ARI, clearly defines abusive behaviour, identifies particular types of abusive behaviour and the mitigation response that ARI will initiate when abusive behaviour is determined. ARI will, owing to their extensive industry experience and established anti-abuse operations, implement and manage on our behalf various procedures and measures adopted through this policy. This robust policy and procedure framework, which will be continually improved, updated and rigidly enforced, will preclude abusive registrations from being made.

Despite utilisation of ARI's anti-abuse service we are nonetheless cognisant of our responsibility to minimise abusive registrations and other activities that have a negative impact on Internet users in our TLD. In recognition of this responsibility, we will play an instrumental role in overseeing the implementation of the anti-abuse service by ARI, as well as having contractual commitments in the form of SLA's in place 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' [http://www.icann.org/en/news/correspondence/aba-bits-to-beckstrom-crocker-20dec11-en.pdf] (the 'BITS Requirements). We acknowledge that these requirements were developed by the financial services sector in relation to financial TLDs, but nevertheless believe that their adoption in this TLD (which is not financial-related) results 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 will implement to minimise abusive registrations and other activities that affect the rights of trademark holders, are specifically described in the response to Question 29.

2 ACCEPTABLE REGISTRATION AND USE POLICY

In consultation with ARI we have developed a comprehensive Acceptable Registration and Use Policy, which is the main instrument that captures our strategy in relation to identifying and handling abuse in our TLD. This is consistent with Requirements 3 and 4 of the BITS Requirements. Because all domain names will be registered to and maintained by us in our capacity as Registry operator, the Acceptable Registration and Use Policy applies solely to us. However, the mitigation response described in the policy will be implemented by ARI. Any breach of the Acceptable Registration and Use Policy by an employee will be considered as a breach of the relevant employee's employment conditions. Any breach by an Affiliate will be handled in accordance with the Acceptable Registration and Use Policy. The mitigation of any such breach, as described by the policy, will be implemented by ARI.

2.1 Definition of Abuse

Defining abusive behaviour by reference to the stage in the domain name lifecycle in which the behaviour occurs presents difficulty because a particular type of abuse may occur at various stages of the life cycle.

With this in mind, we have 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.

Abusive behaviour in a TLD may be defined as 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.

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.

It should be noted that this definition of abuse serves to inform us and clarify certain behaviours, specific to domain names that may cause harm. However malicious conduct of any kind relating to the use of IT resources, which includes the TLD, is strictly against company policy and does not rely on the wording contained herein. Put simply, an abusive or malicious act is against our organisation's documented standard of acceptable behaviour and will be dealt with technically within the registry and directly with any employee or Affiliate.

2.2 Aims and Overview of the Acceptable Registration and Use Policy

Our Acceptable Registration and Use Policy will put those registering and using domain names on notice of the ways in which abuse will be identified and responded to, and serve as a deterrent to those seeking to register and use domain names for abusive purposes.

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 ARI and the steps that ARI will take to determine whether the notified behaviour is abusive.
− Identifies the actions that may be taken in response to behaviour determined to be abusive.

The planned single registrant/single user model of this TLD will enable a close working relationship between Registry operator and Registrar and full Registrar awareness of and compliance with our Acceptable Registration and Use Policy. This will be contractually enforceable through our RRA, which will oblige all Registrars to comply with the Acceptable Registration and Use Policy. Our RRA will additionally incorporate the following proposed 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.

We will re-validate our RRA at least annually, consistent with Requirement 10.

2.3 Acceptable Registration and Use Policy

Our Acceptable Registration and Use Policy is as follows:

Acceptable Registration and Use Policy

Introduction:
The abusive registration and use of domain names in the TLD is not tolerated given that the inherent nature of such abuses creates security and stability issues for all participants in the Internet environment.

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 a 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 email 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 websites 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.

– Willful distribution of malware: the dissemination of software designed to infiltrate or cause damage to devices or to collect confidential data from users without the owner's 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 pornography: the storage, publication, display and/or dissemination of pornographic materials.

– 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:

Although we do not anticipate abusive behaviour in the TLD, it may be detected in the following ways:

– By the Registry Operator through ongoing monitoring of all domain name transactions.

– By ARI through their on-going monitoring activities and industry participation.

– By third parties (general public, law enforcement, government agencies, industry partners) through notification submitted to the single abuse point of contact on the registry website or industry alerts.

Reports of abusive behaviour will be notified immediately to the Registrar of record.

Handling of Abusive Behaviour:
When notification of abusive behaviour by the Registry operator or a third party is received, a preliminary assessment will be performed to determine whether the notification is legitimately made. Applying the definitions of types of abusive behaviours identified in this policy, ARI will classify each incidence of legitimately reported 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. 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
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
In the event that we receive specific instructions regarding a domain name from a law enforcement agency, government or quasi-governmental agency utilising the expedited notification process for such agencies, our mitigation steps will be in accordance with those instructions provided that they do not result in the contravention of applicable law.
Note that these expected actions are intended to provide a guide to the 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 action or instruct a Registrar to take action as we deem necessary, in our discretion to:

1. Protect the integrity and stability of the registry.
2. Comply with any applicable laws, government rules or requirements, requests of law enforcement, or dispute resolution process.
3. Avoid any liability, civil or criminal, on the part of the Registry operator, as well as its Affiliates, subsidiaries, officers, directors, and employees.
4. Correct mistakes made by the Registry operator or any Registrar in connection with a domain name registration.
We may place a registration upon Registry Lock, Hold or similar status a domain name during resolution of a dispute. 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.

3 ABUSE PREVENTION AND MITIGATION BY THE REGISTRY OPERATOR

This section of the response describes abuse-related processes implemented by the Registry operator regarding:
– Building awareness of the Acceptable Registration and Use Policy
– Mitigating the potential for abusive behaviour
– Identifying abusive behaviour
Due to the complete control of all registrations made in the TLD that is provided by an exemption to clause 1b of the Registry Operator Code of Conduct, these processes are anticipated to will form the bulk of our efforts to minimise abusive registrations, as they function to control the behaviour of those in a position to engage in such behaviour.

3.1 Awareness of the Acceptable Registration and Use Policy
As mentioned above, the Acceptable Registration and Use Policy will govern the manner in which domain names may be used. Efforts will be undertaken to ensure that all those registering and using in this TLD within the Registry operator's organisation are made aware of the Acceptable Registration and Use Policy. Awareness will be generated by requiring relevant employees and Affiliates of the Registry operator to attend compulsory information sessions which describe the Acceptable Registration and Use Policy and the ramifications of breaching the policy. Following the attendance of the information session, all attendees will be required to execute documentation which states that the employee or Affiliate has read, acknowledged and understood the policy. The Acceptable Registration and Use Policy will be published on the Registry operator's intranet as well as on the abuse page of our registry website, which will be accessible and have clear links from the home page.
It is anticipated that these efforts will place all employees and Affiliates on notice of the applicability of the Acceptable Registration and Use Policy to all domains in the TLD and furthermore 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 those registering and using domain names. We anticipate that the clear message, which communicates our commitment to combating abusive registrations, will serve to minimise abusive registrations in our TLD.

3.2 Pre-emptive – Mitigating the Potential for Abuse
The following practices and procedures will be adopted by the Registry operator to mitigate the potential for abusive behaviour in the TLD.

3.2.1 Mitigating the Potential for Abusive Registrations that Affect the Legal Rights of Others
Many of the examples of abusive behaviour identified in our Acceptable Registration and Use Policy may affect the rights of trademark holders. While our Acceptable Registration and Use 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. Additionally, our registration policy will involve internal procedures to identify and address potential conflicts with others' trademarks before such names are registered. 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.

3.2.2 Increasing Security Awareness

In accordance with our commitment to operating a secure and reliable TLD, we will attempt to improve awareness amongst those registering and using domain names of the threats of domain name hijacking, registrant impersonation and fraud, and emphasise the need to keep registration information accurate. Awareness will be raised by:

– Conducting biannual information sessions describing new and emerging threats and manners in which they may be mitigated.

– Publishing relevant information on our intranet in the form of videos, presentations and FAQ's.

– Developing and providing to those registering and using domains in this TLD Best Common Practices that describe appropriate use and assignment of domain auth Info codes and risks of misuse when the uniqueness property of these codes are not preserved.

The increase in awareness renders us, as the only eligible registrant in the TLD, less susceptible to attacks on our domain names owing to the adoption of the recommended best practices that mitigate the potential for abuse in the TLD.

3.2.3 Registry Operator's Internal Processes that Mitigate the Potential for Abuse

Eligibility, naming and use restrictions will be imposed in this TLD, consistent with proposed Requirements 1, 3 and 4 of the BITS Requirements, and enforced through internal processes that require approvals within established reporting lines and the use of username and password to verify eligibility to register domain names. As described in detail in our response to Question 18, we will be the only eligible registrant in this TLD.

This arrangement grants us a high degree of control and facilitates the implementation of measures to minimise abuse by significantly decreasing the number of individuals capable of registering and using a domain name and thus having the potential to engage in abusive behaviour. This is in contrast to the inherent decrease in control associated with granting multiple and varied individuals the capability to register and use domain names as demonstrated by many existing TLDs. Our planned single registrant/single user operating model precludes the abusive registration and use of domains in this TLD by unauthorised individuals not within our organisation, whilst also providing no incentive for those within our organisation to engage in abusive behaviour given that our brand is inherently intertwined with all uses of domains in this TLD.

Internal processes regarding the registration and use of domains in this TLD are aimed at maintaining the integrity of this arrangement by ensuring that the registration and use of domains in this TLD is restricted to authorised individuals whose use complies with the Acceptable Registration and Use Policy. These internal processes, which include safeguards against allowing for unqualified registration and use of domains in this TLD, are described below.

The primary safeguard against allowing for registrations in violation of eligibility restrictions is the technical incapability of those not authorised by the Registry operator to register domain names in the TLD. We will only authorise the Project Manager to be the Administrative Contact and the IT Manager to be the Technical Contact for all domains in this TLD. The Registry operator will provide and keep current the contact details of the Project Manager and the IT Manager to the Registrar, who will grant these individuals access to an authenticated web portal to register and manage domain names in the TLD. Individual credentials for accessing this portal will be provided to the Project Manager and the IT Manager by the Registrar via alternative sources. In the event that these credentials are compromised, direct communication with the account manager on the Registrar's end is available. Various security measures will be implemented to ensure that only those personnel

authorised to register and update domain names have access to the web portal. These measures are further described in our response to Question 30.

The Registry operator will review the level of access that personnel have to the web portal, ensuring account permissions are relevant to the employee's role as well as removing permissions of an employee promptly upon termination of employment. All domain name registrations will require the approval of the Project Manager who will ensure that the IT Manager is authorised to create the domain name. In addition, the Project Manager will perform a monthly audit of all domain name transactions to verify that all transactions and the use of domains complies with the Acceptable Registration and Use Policy.

This arrangement effectively mitigates the potential for abuse by restricting the capability to register domain names to a small number of trusted and authorised employees under our direct control and establishing various internal controls to that effect.

3.2.4 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. Restricting the ability to register domain names in this TLD to the Project Manager and the IT Manager means that a domain's contacts are well known and accessible by clear and reliable contact details. These employees will be continually made aware of their responsibility to provide and maintain accurate WhoIs information and the potential ramifications of a failure to do so, including termination of their employment. There can only be two parties responsible for abusive registrations, thus identifying them will require little effort from LEA and the ARI Abuse and Compliance Team. ARI will maintain correspondence with multiple points of contact within the Registry operator's organisation including but not limited to the Project Manager, IT Manager and CEO in order to ensure that all relevant stakeholders are keep abreast of important issues as they occur. Published WhoIs information will thus accurately reflect the identity and contact information of the individual who created the domain name in the name of the Registry operator.

In addition, the Project Manager will perform a monthly audit of all domain names registered in the TLD to ensure that WhoIs information is complete and accurate.

3.2.5 Prompt Notification following Mitigation of Abuse

Our contractual arrangement with ARI dictates that in the unlikely event that a domain name is suspended or cancelled due to the implementation of the Acceptable Registration and Use Policy, ARI will promptly notify us. This notification will allow us to amend internal processes to prevent such behaviour from re-occurring. This notification mitigates the potential for abuse by ensuring that we are responsive to internal breaches of the Acceptable Registration and Use Policy whilst simultaneously putting employees on notice of the ramifications of breach.

3.3 Identification of Abusive Behaviour

Although we do not anticipate the identification of abusive behaviour owing to our internal processes to mitigate the potential for abuse, we will rely on the monthly audit of all domain name transactions conducted by the Project Manager as well as notification of abuse to the Project Manager by third parties through alternate communication channels to identify abusive behaviour in our TLD. In the event that an audit reveals an unauthorised domain name transaction or other behaviour indicative of abuse, the Project Manager will notify ARI, who will take the appropriate mitigation response described below.

4 ABUSE PREVENTION AND MITIGATION BY ARI

This section of the response includes ARI's description of the abuse-related processes ARI will implement regarding:
– Mitigating the potential for abusive behaviour
– Identifying abusive behaviour
– Handling abusive behaviour

These processes form part of ARI's standard anti-abuse service and are designed with a multi-registrant model in mind. We have elected to utilise ARI's anti-abuse service to comply with the requirements of Question 28 but do not anticipate relying strongly on these processes owing to our effective internal abuse prevention and mitigation processes described above. Note, however, that the Registry Lock service described below – beneficial in preventing the unintentional transfer, modification or deletion of the domain name – is best provided by ARI as an independent third party to maintain the separation of parties, which underpins the benefit of the service.

4.1 Pre-emptive – Mitigating the Potential for Abuse
The following practices and procedures will be adopted by ARI to mitigate the potential for abusive behaviour in our TLD.

4.1.1 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 those authorised to register domain names, it is recognised that an added level of security may be provided by 'registry locking' the domain name and prohibiting updates thereby preventing 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 of the Registry operator, ARI will:
1. Verify the identity of the authorised representative.
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 the Registry operator indicating the names for which the Registry Lock service was provided in the previous month.

4.1.2 ICANN Prescribed Measures
In accordance with our obligations as a Registry Operator we will comply with all requirements in the Registry Agreement. In particular, we will comply with the following measures prescribed by ICANN, which will be implemented by ARI 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 section 4.1.3).

4.1.3 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 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 section 4.3 – 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.

4.2.1 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.

4.2.2 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.

– Law enforcement agencies (LEA) through a single abuse point of contact (our Abuse page on the registry website, as discussed in detail in '4.3 Abuse Handling') and an expedited process for LEA.
– Members of the general public through a single abuse point of contact (our Abuse page on the registry website).

4.2.2.1 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. While 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 our Acceptable Registration and Use Policy. In addition, information shared regarding practices indicative of abuse will facilitate detection of abuse by our own monitoring activities.

4.2.2.2 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. Complaints may be received from members of the general public, other registries, Registrars, LEA, government and quasi-governmental agencies and recognized 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 our TLD) will be provided to ICANN and published on the Abuse page of our registry website, which will also include:
– All policies in relation to the TLD including the Acceptable Registration and Use Policy.
– Registrant Best Practices.

As such, the SAPOC may receive complaints regarding a range of matters including but not limited to violations of the Acceptable Registration and Use Policy.

The SAPOC will be the primary method by which ARI and the Registry operator 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.

4.2.2.2.1 Notification by Agencies 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 direct channel of communication with the Registry operator 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. 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;

2. All calls to this number will be responded to by the Registry operator's CEO within 24 hours and handled according to the process outlined in 4.3.4 below;

3. Should ARI be notified by LEA of abuse, ARI will request that the notifying agency contact directly the Registry operator's CEO. ARI will promptly notify the Registry operator's CEO of its having been contacted by LEA regarding abuse.

4.2.2.2.2 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 ticket in ARI's case management system (CMS).

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 ARI's Abuse and Compliance Team to be dealt with in accordance with section 4.3 – Abuse Handling.

4.2.2.2.3 Notification by the Project Manager

It is anticipated that notification by the Project Manager of abuse or potential abuse will serve as the primary method by which ARI identifies abuse in the TLD given that such behaviour is likely to be detected by the Project Manager. In the event that the monthly audit of domain name transactions by the Project Manager reveals an unauthorised domain name transaction or other behaviour indicative of abuse, the Project Manager will notify ARI's Service Desk. All such calls will result in the generation of a CMS ticket, which will be forwarded to ARI's Abuse and Compliance team to be dealt with in accordance with section 4.3 – Abuse Handling, below.

4.3 Abuse Handling

Although we do not anticipate the occurrence of abusive behaviour in our TLD owing to the high degree of control inherent in restricting domain name registrations to authorised employees within our organisation, ARI has processes in place to handle abuse once identified. Upon being made aware of abuse in the TLD, whether by ongoing monitoring activities or notification from third parties, ARI's Abuse and Compliance Team will perform the following functions.

4.3.1 Preliminary Assessment and Categorisation

Each report of purported abuse will undergo an initial preliminary assessment by ARI's 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. This will not at this stage 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 falling within the scope of the Acceptable Registration and Use Policy by the application of the definitions provided in that policy. In

order to make this classification, ARI's 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 ARI may take on our behalf 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.

4.3.2 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. ARI will contact the Project Manager, IT Manager and CEO of the Registry operator's organisation to instruct that the breach of the Acceptable Registration and Use Policy be rectified. If the investigation by ARI's Abuse and Compliance Team 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.

4.3.3 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, ARI's 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 Acceptable Registration and Use Policy. Restoration of the domain name will result where further investigation determines that abusive behaviour, as

defined by the Acceptable Registration and Use 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 Acceptable Registration and Use 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, ARI's 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.

4.3.4 Executing Agency Instructions

We understand the importance of our role as a Registry operator in addressing consumer vulnerabilities and we are cognisant of our obligations to assist law enforcement, 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. Sharing all available information upon request from LEA utilising the expedited process, including results of our investigation.
3. Providing bulk WhoIs information upon request from LEA utilising the expedited process.
4. Acting on instructions by the 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 described in 4.2.2.2.1 above, one of the following may occur:

1. The reported behaviour will be notified to ARI and subjected to a preliminary assessment and categorisation by ARI, as described in 4.3.1 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 notifying agency was handled will be provided to us by ARI within 24 hours, for provision to the notifying agency by us. This report will also be recorded against the relevant CMS ticket.

OR

2. Where specific instructions are received from the notifying agency in a format acceptable to the Registry operator's CEO, we will act in accordance with those instructions provided that they do not result in the contravention of applicable law. We will execute the instructions of the notifying agency within 12 hours. Following prompt execution of the request, a report will be provided to the agency in a timely manner.

Finally, whilst we do not anticipate the occurrence of a security situation owing to ARI's 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

The efforts to minimise abusive registrations and other activities that have a negative impact on Internet users in this TLD will be undertaken jointly by employees of the Registry operator and ARI.

5.1 ARI
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 this TLD projects 60 domains, 0.0001% of these resources are allocated to this TLD. 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. Additional trained resources can be added to any of the above teams with a 2 month lead time.

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 for our measures to minimise abusive registrations and other activities that affect the rights of trademark holders are described in our response to Question 29 − Rights Protection Mechanisms.

All of the responsibilities undertaken by ARI's Development Team, Abuse and Compliance Team, and Service Desk are inclusive in ARI's Managed Registry Services fee, which is accounted for as an outsourcing cost and explained in our responses to Question 47. The resourcing needs of these teams have been determined by applying the conservative growth projections for our TLD (which are identified in our answer to Question 48) to the team's responsibilities at start-up and on an ongoing basis.

5.1.1 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

5.1.2 ARI Abuse and Compliance Team

ARI's Abuse and Compliance Team will be staffed by four full-time equivalent Policy Compliance Officers. These roles will entail the following:

A principal responsibility of the Policy Compliance Officers will be handling notifications of abuse through the SAPOC. This will involve identifying and categorising suspected abuse according to our Acceptable Registration and Use Policy and carrying out the appropriate mitigation response for all categorised abuses. Policy Compliance Officers will also be responsible for analysing registry data in search of behaviours indicative of abuse and reviewing industry lists in search of data that may identify abuse in the TLD. Furthermore, Policy Compliance Officers will provide training to the Project Manager of the Registry operator's organisation regarding abuse prevention and mitigation in order to enable the Project Manager to competently manage the registration and use of domain names and conduct information sessions which highlight the application of the Acceptable Registration and Use Policy.

Policy Compliance Officers will act on the instructions of verified agencies or 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 Registry operator's CEO 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.

5.1.3 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 Acceptable Registration and Use Policy.

For more information on the skills and responsibilities of these roles, please see the in-depth resource section in answer to Question 31.

5.2 Registry Operator

The following is a description of the resources that are allocated to performing the tasks required by the Registry operator. These tasks will be absorbed by the individuals currently performing the following roles within the Registry operator's organisation.

5.2.1 Project Manager

In the context of operating this TLD the Registry operator's existing Project Manager will be responsible for managing the creation of all domains in this TLD. The Project Manager must pre-approve all requests to create and/or update domain names by the IT Manager. In addition, the Project Manager will perform a monthly audit of all domain name transactions to verify that they were authorised and that the use of the domain name complies with the Acceptable Registration and Use Policy. The Project Manager will review the level of access that personnel have to the web portal, ensuring account permissions are relevant to the employee's role as well as removing permissions of an employee promptly upon termination of employment. Finally the Project Manager will conduct biannual information sessions to improve awareness of the threat of domain name hijacking and fraud as well as raising awareness of the Acceptable Registration and Use Policy.

5.2.2 IT Manager

The Registry operator's existing IT Manager will be responsible for managing the Registry operator's domain name portfolio, which will involve creating, updating and maintaining all domains in this TLD in the name of and for the exclusive use of the Registry operator.

5.2.3 CEO

The Registry operator's existing CEO will be responsible for responding to all reports and requests by LEA and managing the expedited process for those agencies and handling all escalated complaints and 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, resolving disputes and liaising with all relevant stakeholders (Registrars, registrants, LEA, general public) as needed in fulfilling these responsibilities.

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