New sTLD RFP Application

.mail

Part B. Application Form

Name and Address fields

Company/Organization Information

Company Name	N/A
Company Address 1	N/A
Company Address 2	N/A
Company City	N/A
Company State/Province	N/A
Company Postal Code	N/A
Company Website Address	N/A
Company Country	N/A

Sponsoring Organization Information

Sponsoring Organization Name	The Anti-Spam Community Registry
Sponsoring Organization Address 1	TBD, but for now use: Phoenix
Sponsoring Organization Address 2	TBD, but for now use: Taggs Island
Sponsoring Organization City	TBD, but for now use: London
Sponsoring State/Province	TBD, but for now use: The Hamptons
Sponsoring Organization Postal Code	TBD, but for now use: TW122HA
Sponsoring Organization Country	TBD, but for now use: UK
Sponsoring Organization Website Address	TBD, but for now use: www.spamhaus.org

Namestrings and Conventions

First sTLD choice:	.mail
Naming Conventions:	
The names registered will be of the form "key.mail" where "key" is of the form "sld.tld" and where "tld" is an ICANN top-level-domain with certain attributes and where "sld" is a second-level-domain which is already registered in "tld". The registrant of the "key" domain must be the same as for "key.sTLD"	

Second sTLD choice:	.tmail
Naming Conventions:	
The names registered will be of the form "key.tmail" where "key" is of the form "sld.tld" and where "tld" is an ICANN top-level-domain with certain attributes and where "sld" is a second-level-domain which is already registered in "tld". The registrant of the "key" domain must be the same as for "key.sTLD"	

Third sTLD choice:	.mta
Naming Conventions:	
The names registered will be of the form "key.mta" where "key" is of the form "sld.tld" and where "tld" is an ICANN top-level-domain with certain attributes and where "sld" is a second-level-domain which is already registered in "tld". The registrant of the "key" domain must be the same as for "key.sTLD"	

Sponsoring Organization Structure

The Sponsoring Organization (SO) represents the community of individuals and companies who wish to receive spam-free email and individuals and companies who wish to send spam-free email and who do not want to be blocked, filtered or inconvenienced when doing so. The proposed sTLD will be limited for use by the registrant only during the process of sending email.

The function and mission of the Sponsoring Organization is solely to set policy and rules for the names in the TLD and to deny entry into the zone or to remove those names from the zone that violate those set policies and rules. The policies and rules are designed to insure the community that emails sent using domains in this sTLD can be trusted to be spam-free.

The SO will be a not-for-profit organization. The name of the SO is “The Anti-Spam Community Registry”. The SO will sub-contract to the Registry Operator (RO) all of the typical registry operations (registration, zone file generation, etc). Because this proposal requires extra-registry services, the SO will also subcontract another organization to perform these non-typical services. We are calling that organization the “extra services operator” (XO). Both the RO and XO are existing for-profit companies with many years of experience in the Internet and domain name industry. Details of the duties and capabilities of these organizations are presented later in the proposal.

Since the SO represents the community of senders and receivers of spam-free email, it will consist of a board of advisors who each represent parts of this community.

For example, The Spamhaus Project, the founding member of the SO, represents a very large number of organizations who, by virtue of their using the Spamhaus Block List (SBL), have endorsed Spamhaus' ability to aid them in determining which email is spam and which is not. The SBL is used on approximately 200,000,000 email accounts worldwide, on millions of domains. Looking at these numbers and the fact that the blocklist receives over one billion queries per day (not counting the high-volume users who transfer the zone and query it locally) Spamhaus, by itself, represents a very large segment of the community. This community will be represented on the SO board by Steve Linford, the founder of Spamhaus, and who was recently named by the ISPA (The Internet Service Providers Association of the UK at ispaawards.org.uk) the "United Kingdom's Internet Hero of the Year in 2003" for his tireless work in helping define responsible emailing practices and encouraging the Internet community to implement systems to make it so.

All the board members will use their knowledge in their particular fields to create and modify the policies of the sTLD using the procedures of policy development of the SO. Special advisors will also be used from time to time to advise the board on relevant topics, to recommend policies and to recommend additional board members from their field of expertise.

Spamhaus personnel will help populate the staff of the SO, and will, on a daily basis, be the ones to validate and enforce the sTLD's stated responsible email policies. They will use the technology and tools provided by the XO and the RO, combined with their expertise, and the policies of the SO, to accomplish this task.

This sTLD will have all customary policies which apply to all other ICANN gTLD registries, for example deletes and RGP. The board will oversee the email-specific, whois-specific polices and other policies that make this TLD unique. The SO will follow all ICANN directives and will not offer any other registry services that are not detailed in this proposal or that do not assist in the mission of the SO. The SO, using 1) the rules, policies and procedures outlined in this proposal (rules such as each name must have validated whois contact information, and must have messages sent to abuse@key.sTLD received by the SO, not the registrant) and 2) their knowledge of responsible emailing practices and 3) their knowledge of those specific individuals and organizations who violate those practices, will determine which domains are accepted or removed from the zone. Much in the same way that Spamhaus' SBL has, over the past years, gained the trust and acceptance of a large segment of the world's email providers so that it is now protecting an estimated 40% of all active email accounts, the similar activities and participation of Spamhaus will help the SO insure the trust and acceptance of this sTLD by the same large segment of the world's email providers (senders and receivers).

The SO's policy enforcement operations are carried out on a daily basis as is required by the very mission of this sTLD, primarily centered around adding names to the zone that comply with the policy and removing names from the zone where the registrants have violated the policy.

Policy-formulation and modification activities will consist of quarterly meetings, either in person or by teleconference, of the board of advisors and other experts when needed. These meetings will take as input an SO-maintained publicly accessible email list where suggestions to improve the implementation of the mission of the sTLD will be solicited. Unlike a gTLD, the SO, due to the sTLD's designed technical structure, is in a unique position to receive all abuse messages for each domain. These messages are submitted to the SO from a part of the community this sTLD represents (mail recipients). These abuse messages, in aggregate (besides each being used in the daily operation of the sTLD policy enforcement), will be used by the board to both insure the operation of the sTLD is following its stated polices and to aid in refining policies where the need arises.

Appropriateness of Sponsored TLD Community

The Sponsored TLD Community is defined as responsible senders and receivers of spam-free electronic mail.

The Sponsored Community, although large, does not include senders of spam. For the purposes of this community, the definition of spam is an electronic message that is considered to be Unsolicited Bulk Email ("UBE").

(1)Bulk means that the message is sent as part of a larger collection of messages, all having substantively identical content, of which the recipient's personal identity and context are irrelevant because the message is equally applicable to many other potential recipients; AND
(2)Unsolicited means that the Recipient has not verifiably granted deliberate, explicit, and still-revocable permission to receive the message.

A message is defined as spam only if it is both Unsolicited and Bulk. This distinction is important because either unsolicited email or bulk email, on their own, is not classified as spam under this definition.

* Unsolicited Email is not spam (examples include first contact enquiries, job enquiries, sales enquiries, etc.)

* Bulk Email is not spam (examples include subscriber newsletters, discussion lists, information lists, etc.).

Many people suffer the costs of spam which includes wasted time, wasted capacity (cpu, bandwidth and storage), wasted manpower, hassle and aggravation. These people (who receive spam) have in front of their email client a mail server that receives email. The operator of this receiving email server and the operator of the server that sends the email are the core community of technical people for which the sTLD is intended. The sTLD is designed for mail server operators who follow “the rules” to be able to identify each other. The sending server operator registers a name in the sTLD and the receiving server operator uses the DNS to lookup information (IP address and other information) about the name and hence the sending server. Using this information, the receiving server can easily determine if the sending server is spam-free, as well as determine if the email was forged. Also, using this sTLD, this community (these technical people to a large extent, but also the public) can send abuse messages to the domain and be assured that their message will not be ignored because all abuse messages are received by a third-party (the SO), not by the suspected abuser.

No email messages will be seen to come from the sTLD, so that the public (the non-technical people using email) will not know that the mail servers used the sTLD. These people will see no change whatsoever in the email in their inbox. The domains in the “from”, “to”, “reply-to”, and other data elements of the email header will not include domains in the sTLD. The sTLD is behind the scenes. The public will continue to see, for example, the domain “example.com” being used. However, as the sTLD becomes better known to the public, they will become aware that they can simply type “example.com.mail” or "www.example.com.mail" (just add the easily remembered ".mail" to the end of any domain) into their browsers at anytime to obtain information regarding the registrant and its email practices, or to send abuse mail simply use "abuse@example.com.mail".

Law enforcement, internet service providers and the intellectual property communities are also served due to the fact that all the whois information for each sTLD domain is validated and carries a paper trail (of postal address and email confirmation). This accurate whois verification benefit will also now apply to all the other TLDs, for example “.com”, due to the fact that the registrant of “example.com.mail” is the same registrant as “example.com”.

As more and more receiving mail server operators, MTA (Mail Transfer Agent) programs, and email policy programs (email filters) learn that mail sent using the sTLD is spam-free, it will build trust in the sTLD so that more operators will obtain domains in the sTLD and will let the spam-free mail pass unencumbered.

Therefore, the sTLD’s main community is those core technical people who operate mail servers that send and receive email, while the sTLD also serves the much wider community.

The benefit to the broader community is that this sTLD facilitates the unencumbered delivery of spam-free electronic mail communications for those members of that community that choose to use it either directly or indirectly.

The community of email senders and receivers is long-lasting because email is here to stay. People all over the world send email. It is geographically independent. Sadly, the desire and ability of a segment of mailers to send spam will be with us as long as email exists. This sTLD can greatly help solve the major problem of this community; and because the SO generally represents this community, then this sTLD is worthy of delegation to the SO for the purposes of helping to solve the problem.

Representation

The SO represents the community because each member of the board represents different sub-communities within the sponsored community. It is self evident that each of these communities has an interest in the unencumbered flow of spam-free email and as such are all stakeholders.
These sub-community categories are:

1) The community comprised of anti-spam advocacy groups and individuals
2) The community comprised of individuals and companies involved in the creation of email-policy programs (anti-spam email filter software) and systems.
3) The community comprised of individuals and companies involved in the creation of email server software and systems
4) The community of university based network and email systems researchers
5) The community of internet service providers and large mail recipients

Each board seat will represent one of these sub-communities, for a total of five board seats.

Special advisors who may also provide input or expertise to the SO may also be selected from time to time. These will be people who are active in the

Anti-Spam, email server, email policy, ISP, or spam-research arenas or from the broader Internet community.

The following five entities are examples that the proposers believe could contribute individuals, well known to the community, who would represent the above five sub-communities at the SO board level:
1) Spamhaus.org, a worldwide anti-spam advocacy group based in the UK that is trusted to protect over 200 million email accounts (estimated to be 30-40% of the world's active email boxes)
2) SpamAssassin, the creators of one of the most popular email policy program (email filter)
3) Sendmail, a leading mail server software
4) University of Oregon, a leading spam research institution
5) Outblaze.com, the world's leading outsourced email provider

To date, not all of these entities have committed to participate at the board level. Please refer to "Part B Application Form Initial Directors, Officers and other Staff" for the list of board members and special advisors.

Since the goal of this sTLD is to aid in the unencumbered transmission of spam-free email and to benefit email messaging into the future, input from the community will be a vital and an integral part of the SO.

Input Mechanisms
1) An email list (discussion forum) will be setup so that any and all people who consider themselves members of the community can easily communicate their thoughts, ideas, suggestions, improvements and comments which the board will review and make policy modifications based on this input. The messages on the email list will be made public via an SO website.
2) Also, a unique attribute of this sTLD is the input channel afforded to the community by the implementation of a centralized email abuse messaging system. Because the SO controls the name server records for every domain, it will place an MX record for each domain in the name servers, and this MX record will point to a mail server under the control of the SO, and in the mail server the SO will setup an “abuse” (and "postmaster" required by RFC 2821 & RFC 2142) account for each domain. Therefore, the SO will receive all abuse messages for every domain sent by the broader community. This input will be used in two ways, first, on a daily basis to help determine any violations of the policies of the sTLD, and second, as input, in aggregate, to the board of the SO to help them determine future policy changes.
3) Polling will also be used to gauge the community on various issues of interest
4) The special advisors will also provide input in their areas of expertise

Informational services:
1) Each domain’s website will be controlled by the SO. These sites will display information regarding the registrant, for example, the registrant’s contact information that was verified by the SO.
2) On the main SO website, there will be information regarding implementation of the sTLDs system across the entire spectrum of technology expertise. For example, how to use the sTLD with mail servers such as Sendmail, Exchange, QMail, or Postfix, email policy enforcement software such as SpamAssassin and “how-to” information for registrants as well.
3) The main SO website will also contain areas to provide up to date information on activities regarding the sTLD.

In summary, we will provide the following community communication mechanisms:

1) Public open discussion forum
2) Abuse messages.
3) Polling and Special Advisors
4) Registrant’s informational website.
5) “How-to” informational website
6) Updates informational website.

Openness and Tansparency

The founding member of the SO, Spamhaus, has been a proponent of openness on spam issues since its inception in 1998, and will insure this tradition continues at the SO. The Spamhaus.org website is probably the most referenced repository of information on spam issues and spammers. Spamhaus has felt that openness and transparency helps the people who know there is a problem identify the causes of the problem and the possible solutions.

The SO will allow public access to all meeting minutes. Comments on policy changes will be welcome and the input will be used to refine the policies where needed. The goal of this sTLD is to best serve the needs of the responsible emailing community and the SO acknowledges that the input from the community is the most important factor in determining how to implement and make changes to the system and its policies in the future.

The SO will post public notice on the SO website explaining what policies are being considered for adoption and why. It will provide a reasonable opportunity for parties in the community to comment on the adoption of the proposed policies, to see the comments of others, and to reply to those comments.

The following types of information will be published:
1) On the main SO website:
a. Mission statement of the SO
b. The policies of the SO and the sTLD registry
c. Detailed instructions and a FAQ on what is needed to obtain a domain in the sTLD
d. Detail technical documentation on the correct usage of the domain to email applications.
e. Board meeting minutes
f. Updated archive of the public forum email list
g. Latest events and news regarding the sTLD which would include changes and additions to the board, links to stories in the press, etc.
h. The ICANN accredited registrars who are certified to make registrations in the sTLD with links to their websites.
i. An admin tool for certified registrars and instructions on how to obtain certification for ICANN accredited registrars.

2) On the registrant website:
a. Verified contact information for the registrant
b. Current status of the domain, for example if the domain has been removed from the zone for a policy violation, a count of the number of days until the registrant can reapply.
c. Abuse reporting procedures and addresses
3) The zone file
4) Whois information, via web and port-43 that follow all ICANN and IETF specifications and directives

There may be certain details in the policies concerning the detection of violations process that the SO will not make public because knowledge of the underlying methodologies can be used by spammers in an attempt to circumvent detection.

Initial Directors, Officers, and Other Staff

The initial board of directors will consist of:

Steve Linford, founder of Spamhaus.org, Representing Anti-Spam Advocacy.

Linford was born in England. After moving to Rome and dropping out of photography school, Steve purchased a motor home, parked it on beaches and made his living by playing guitar in coffee shops. When artists such as Pink Floyd toured Italy, Linford served as their road manager.
In 1986, Linford drove his motor home to England where he set up a company with the purpose of putting musical tours online. Then Linford started a web page design and hosting business, called Ultradesign Internet. After getting fed up with receiving spam, he became an anti-spam activist. In 1998, he started the Spamhaus project. Currently his spam list is used by many Internet providers that collectively serve more than 200 million email accounts.
Hero of the anti-spam movement, Steve Linford is a man on a mission. His Spamhaus organization identifies and tracks the worst bulk emailing offenders and works with ISPs to block their incessant traffic. Testimony as to how successful he's been comes from an unlikely source - the spammers themselves. His message is clearly getting through - and as a result, theirs aren't.

Joseph E. St. Sauver, Ph.D. Representing University Based Network and Email Systems Research Community

Dr. Sauver is the Director, User Services and Network Applications (since 1987) at the University of Oregon. Dr. Sauver manages 17 professional staff plus numerous part time student employees. Examples of his recent research/writing/presentation work include:
* "The Open Proxy Problem: Should I Worry About Half a Million Trivially Exploitable Hosts?" NLANR/Internet2 Joint Techs, August 2003. Following that presentation and related efforts, the FTC announced creation of Operation Secure Your Server (January 29, 2004)
* "Practical Issues Associated with 9K MTUs" NLNAR/Internet2 Joint Techs, February 2003, Following that presentation and related efforts, the Federal JET adopted a public policy endorsing increasing the MTU on the federal mission networks (DREN, ESNET, NISN/NREN, etc.) to 9000 bytes.
* The November 2003 issue of Network Analysis Times (the issue distributed at Supercomputing) included his piece regarding IPv6 measurement initiatives he is involved with
* The March 2004 printed and online edition of Syllabus Magazine featured his article, "What Are Portalized University Home Pages Rare?"
* Invited to facilitate the October 2003 NWACC Single Sign On Workshop at Reed College
* Presentation "Winning the War on Spam" for NWACC in June 2003
* Invited to speak at the 2004 Cornell/Educause Institute for Computer Policy and Law
* Dr. Sauver was invited to sit on, and participate in the Internet2 Abilene Network Technical Advisory Committee as well as a variety of other Interne2-related groups such as the new SALSA (Security at Line Speed) advisory group.
Dr. Sauver also performs private consulting for a variety of ISPs and government agencies.

At the time of this application, three board seats are yet to be filled.

Once this proposal is communicated to the wider community, we expect members of the community to step forward and express their willingness and qualifications to serve. The existing board members will also actively recruit additional candidates from the following non-exhaustive list:

John Levine
Chairman of the Anti-Spam Research Group (ASRG) of the Internet Research Task Force (IRTF)
The IRTF focuses on longer term research issues related to the Internet. Since late 2003 John has been co-chair of the Internet Research Task Force's Anti-Spam Research Group (ASRG, asrg.sp.am). He has re-chartered the ASRG, established informal contacts with large Internet providers, and set up new working groups. Since 1997 he's been a board member of the Coalition Against Unsolicited Commercial E-mail (CAUSE, cauce.org), a user advocacy group. He also runs the Network Abuse Clearinghouse (abuse.net), a popular free service that helps Internet users report and deal with on-line abusive behavior. John has written or co-authored over twenty books, from the best selling Internet for Dummies, now in its ninth edition, to technical works on compiler and graphics software.

Wietse Zweitze Venema, Ph.D.
A lead technologist behind Postfix
Most people know Dr. Venema from software that he wrote to protect systems against Internet intruders. He continues this fine tradition with IBM, at the Thomas J. Watson Research Center, in the USA. The first result is Postfix. This is mail server software that aims to be fast, easy to configure, and has a reputation as being very secure. A second result is the Coroner's Toolkit, written with Dan Farmer, primarily for the post-mortem analysis of computer break-ins. Dr. Venema was awarded with the SAGE 1999 outstanding achievement award, and with the NLUUG Award 2000 in recognition of outstanding achievements for the users of UNIX and Open Systems. In June 2002 he reached the legal limit on his term as chair of the FIRST, an international association of computer security teams with over 100 members world-wide in government, industry, and academia. Previously he studied physics at Groningen University in the Netherlands, where his Ph.D. dissertation was on work done at the KVI. He spent 12 years at Eindhoven University, the Netherlands, as systems architect at the Mathematics and Computing Science department. For 8 years, part of that time was devoted to writing tools for automated translation of EDI (Electronic Data Interchange) messages.

The two preceding candidates have already consented to be special advisors to the SO

Justin Mason or Daniel Quinlan of SpamAssassin.org
SpamAssassin, representing the most widely used open source end-user email policy enforcement software, is also participating in the SO. Based on SpamAssassin’s wide use and acceptance they are both well suited to represent the even wider constituency of email policy (spam filter) users on the SO board of advisors.

Eric Allman of Sendmail.org
Sendmail, representing the most widely used mail server software (MTA mail transport agents) would be a good candidate. Based on Sendmail’s wide use and

acceptance, Eric Allman is well suited to represent the even wider constituency of email mail server users on the SO board of advisors.

Ted Galvin of SpamCon.org
SpamCon.org is one of the primary anti-spam advocacy groups. Ted's presence would be to insure that anti-spam advocacy group's voices are heard.

Suresh Ramasubramanian of OutBlaze.com
Manager, Outblaze Security & Antispam Operations and Coordinator, CAUCE Asia Pacific (APCAUCE)
Suresh's presence would be to insure that both large email service providers and the international anti-spam advocacy group's voices are heard.

SpamAssassin and Sendmail can help the world-wide implementation of the gTLD system by modifying their systems to allow mail using domains in this sTLD to pass in an unencumbered manner to the recipients.

CAUCE.org and SpamCon.org, in their normal advocacy endeavors, will help popularize the ideas behind this proposed system (and sTLD) to ensure the delivery of responsible email.

SO Staff
The SO staff will be supplied by the Spamhaus organization. Currently there are twenty members on staff at Spamhaus. These staff members, who are located in a number of countries spanning several continents, are highly qualified in the field of spammer identification and crafting responsible email policies due to their many years of experience in the field. Many have advanced degrees and detailed technical knowledge of DNS, mail and other protocols. The members of the staff have existing contacts with law enforcement including The US Secret Service, The Federal Trade Commission, The FBI, The SEC, The IRS, Scotland Yard, Interpol, and many US State Attorneys General and local law enforcement. Spamhaus staff members also have been at the forefront of legislative activities regarding spam with various governments. In their current everyday duties they also interface with network administrators from all tier-1 and many other tier Internet service providers.

Selection of Directors, Officers, Members, Staff

Each director must have a long history of service in the sub-community that they represent and must have overwhelming respect of their peers. The five sub-communities are:

1) The community comprised of anti-spam advocacy groups and individuals
2) The community comprised of individuals and companies involved in the creation of email-policy programs (anti-spam email filter software) and systems.
3) The community comprised of individuals and companies involved in the creation of email server software and systems
4) The community of university based network and email systems researchers
5) The community of internet service providers (or large email recipients)

The initial board has been selected, except for a representative from the ISP sub-community. Any vacant seats, whether by removal or resignation, will be filled by nomination and election by the current board. There is no geographical diversity requirement as to the board member’s home country location. The SO believes diversity of geographical locations is beneficial but also seeks the best qualified candidates that represent the various sub-communities. Candidates must be nominated and seconded by two different board members. Vacancies will be filled within three months of the vacancy. The nominees must carry 2/3 of the vote of the members in order to be elected. All voting may be conducted electronically. Spamhaus, as the founding member, and representing the anti-spam advocacy group with over 40% of all email boxes deferring to their judgment, has a permanent seat and cannot be removed, and receives an additional vote during votes that result in a tie. A board member can be removed by a 2/3 vote of the other members. As discussed, below, changes in the number of board members may only be made by a change to the Articles of Incorporation, which would require a 2/3 vote of the members. The initial term of service is the same as the initial term of the contract. Any board member who wishes to resign must submit a letter of resignation to the board.

Directors, board members, officers, and staff have a duty to recluse themselves from any votes or decisions where there is a conflict of interest. Each board member, officers, and staff, must disclose any material fact that may be interpreted as a conflict of interest. The board or committees of the board may take action from time to time to appoint officers and staff, following the procedures outlined below in the section titled "Policy-Making Process."

Compensation will be commensurate with directors at similar non-profit organizations.

Meetings and Communication

The board will meet at least once per quarter. Meetings can take place by teleconference or in person. The date, time and location of these quarterly meeting will be communicated to all board members at least 30 days before the meeting. The board can call other teleconferencing meetings with a 2/3 vote, if desired. Minutes will be taken by an SO staff member and made available at the SO website within 10 working days from the end of the meeting.

Fiscal Information

The Sponsoring Organization is newly formed. We estimate an initial SO staff of 2 (before delegation is made) will be required. We project this to increase to 7 in the first year and 16 in the second. These staff members will be mostly coming from Spamhaus’ existing staff and augmented by new hires. Please see the business plan and the financial model for estimation on the annual revenue and costs.

The RO is a public company and has an existing staff of over 3,200 employees, and the XO has an existing staff of over 50 with revenues of over $25 million.

Indemnification from Liability

It is anticipated that, with respect to indemnification from liability, the SO will follow the contractual example set by other registries. The SO will enter into a registry agreement with ICANN. ICANN accredited registrars will (or have already) entered into Registrar Accreditation Agreements (“RAA’s”) with ICANN. Those Registrars that wish to sell domain names in the sTLD will enter into an RAA appendix (“RAA Appendix”) with ICANN as well as a Registry-Registrar Agreement (“RRA”) with the SO. These documents will follow accepted industry language with respect to the following:

• Registrars shall be required to defend and hold harmless ICANN, the SO, the RO, and the XO, (including employees, directors, officers, representatives, agents, shareholders, and affiliates of all such entities) against any cost (including court costs and attorney fees) claim, suit, action, or other proceeding brought against such parties relating to any product or service of the registrar, relating to any agreement between a registrant and a registrar, or relating to the registrar's domain name registration business (including fees, advertising, customer service, and other business practices). There will also be a limitation of liability provision precluding special, indirect, incidental, punitive, or consequential damages, and limiting the SO's, the RO's, and the XO's damages with respect to the registrars to be no greater than specified performance credits to be granted should certain defined circumstances occur. The registrars will be required to bind the registrants to substantially identical indemnification and limitation of liability provisions, except that the limitation of liability (in addition to precluding consequential damages, etc.) shall limit liability to registrants to no more than the amount paid by the registrant for the Compliance Review and Monitoring Service Fee.

• Registrars shall be required to carry insurance in the amount of $1,000,000.00 to ensure the registrars ability to meet the requirements of the indemnification provisions and to protect the named parties in the event that the registrar fails to bind registrants to some or all of the required terms.

• Registrars shall be required to implement the policies of the registry and the policies established by ICANN with respect to WHOIS, UDRP, transfers, and such other policies as may be established through ICANN's consent procedures from time to time; however, there will be the special requirement that the WHOIS, UDRP, and other decisions with respect to the Key Domain(s) shall apply to domains in this sTLD.

• The precise language of the RRA and RAA Appendix will follow the form of language found in agreements such as the .us Registry-Registrar Agreement.

• Contracts relating to this sTLD will include additional language requiring that registrars require registrants to agree to the following terms:
a) Registrants shall acknowledge that they have no property rights in domain names in this sTLD and to acknowledge that the listing of domain names in this sTLD is strictly a service;
b) The registrants will be required to acknowledge that the SO has the sole and complete discretion to evaluate the registrant's application and continued compliance with the sTLDs policies according to criteria established by the SO, criteria which, similarly, are the sole and complete province of the SO to establish and modify from time to time;
c) The registrants will be required to agree to the following arbitration related terms: to binding arbitration in the jurisdiction of the SO regarding any dispute relating to interpretation of the service agreement; that the decision of the SO regarding the listing or de-listing of a domain name in the zone would remain undisturbed during the pendency of the arbitration proceeding; that each party would have to bear its own costs in the arbitration up to the point of the decision; that the looser in the arbitration would have to pay the costs of the winner, up to a specified cap; and that both parties would have to post a bond sufficient to ensure payment to the winner.

Because of the unique nature of this proposed sTLD, in which registration of the Key Domain in another TLD is a pre-requisite, many of the legal and liability concerns which relate to other TLDs do not apply to this sTLD. For example, UDRP arbitration proceedings would never take place with respect to domain names in this sTLD because the WHOIS listings as well as the management control of domain names in this sTLD would follow the designations established by UDRP, judicial, or other proceedings which apply to the Key Domain in the other TLD.

Because of the unique functional nature of this proposed sTLD, there will be complaints surrounding the de-listing of domains from the zone of this sTLD. For the reasons discussed below, this leads to the requirement for the arbitration process, referenced in paragraph c), above, which is unique to this sTLD.

In terms of complaints regarding de-listing actions (or refusals to list a domain in the zone), the complaining party would have contractually agreed that the SO was the sole and complete authority, both with respect to evaluating the registrant's application and with respect to establishing and modifying the application criteria. However, when a first party pays money to a second party in exchange for which the second party evaluates the first party according to some criteria and then makes the results of the evaluation available to third parties, then a claim can arise that the payment of money in exchange for the evaluation creates an illusory contract unless the evaluation criteria can be determined. If the evaluation criteria cannot be determined, then a court would not be able to inquire as to whether or not the promised evaluation took place. If a court agrees that the evaluation criteria are too indefinite to form the basis of a contract, then one remedy might be to allow the registrant to void the contract and obtain a refund of the Compliance Review and Monitoring Service Fee. However, it is likely that a court would look to statements made by the SO to third parties who are meant to convince the third parties to use the sTLD as a basis for accepting or rejecting email and that the court would use such statements as a basis for performing its own review of the evaluation criteria. Under such a scenario, a court might review the determined evaluation criteria, notwithstanding contractual claims that the evaluation criteria are the sole province of the SO, and order that the Court's interpretation of the evaluation criteria be adopted by the SO. Thus, under "worst case" scenarios, potential outcomes would be either a rescission of the contract and a refund of the Compliance Review and Monitoring Service Fee or the imposition of the court's judgment regarding the court's own determination of the evaluation criteria (as the court finds these in statements made to third parties).

To avoid this potential, remote as it may be, the language providing for binding arbitration is to be included in the terms and conditions imposed on registrants, as well as language limiting damages to the amount of the Compliance Review and Monitoring Service Fee. It is tempting to adopt processes such as those defined in the usTLD Nexus Dispute Policy and Rules, which, in many respects, are similar to the UDRP arbitration rules. However, spam is different from a trademark context, or even a .us nexus context, requiring departures from the approaches of the UDRP or the usTLD NDPR. The primary difference in the context of spam is that victims of spam individually suffer a small harm from any one spammer; as a consequence, victims of spam are insufficiently motivated to assume the cost of mounting an arbitration proceeding against the spammer(s). Under both the UDRP and the usTLD NDPR, the complaining party must pay the cost of initiating the arbitration proceeding – typically between $1000 and $1500 (US). Also in the context of spam, action would have to be taken immediately by the SO to de-list spammers. If a third party victim, such as an individual email user or an ISP, were required to initiate an arbitration proceeding as a condition precedent to shutting down spammers, then spammers could rapidly move to new domains with the sTLDs, effectively circumventing the function of the sTLD and thereby destroying the value of the sTLD for its community.

As a consequence, the decision to de-list a registrant from the sTLD must be made rapidly and the ultimate responsibility for the decision must rest with the SO. The principal of “looser pays” in the arbitration proceeding protects registrants who may be de-listed without a substantial basis and it protects the SO from disingenuous challenges. The requirement of a bond ensures recovery under the “looser pays” principal. The commercial bonding industry creates an economically efficient third-party private evaluation of credit worthiness and risk, which moderates the burden of the bonding requirement based on private, competitive, evaluation of such risk factors as the bonding company believes are relevant. As an example, if a legitimate company with low risk factors feels that it has been de-listed by the SO without justification, then a private bonding company would be willing to put up the bonded amount with payment of a relatively low price, such as 10% of the bonded amount. A company presenting high risk factors and/or a weak claim would have to pay a higher amount to convince a private bonding company to put up the bonded amount.

Proposed Extent of Policy-Making Authority

The need of the community that the SO represents is to send and receive spam-free email. The scope of the policy-making authority requested by the SO is tailored to fit this need of this community.

The policy decides who may register in the sTLD and under what circumstances the registration may be revoked. The SO seeks complete authority in disallowing and removing names from the zone at anytime for violations of policy. The limits of the policy formation authority are in the area of preventing spam and insuring that the sTLD is trusted. “Trusted” means, for example that the whois information is trusted to be valid and verified and that messages sent using the sTLD are spam-free.

To illustrate, the following are three examples:
1) Because there is no need for the registrant to point the domain name to a particular website, we are seeking the authority to point them all to a site controlled by the SO
2) Because there is a need for a third party to receive the abuse mailbox messages, we ask that the SO have authority over each domain’s name server pointers and the MX records therein so that all abuse messages are sent to the SO.
3) Because an especially large need of the community is for each domain in the zone to have accurate and trusted whois, we will be validating each whois record before granting use of the sTLD domain.

The SO will have complete authority in determining the namespace in which domains may be registered for this sTLD. Initially, names will only be allowed to be registered in the format, KEY.sTLD, where KEY is an already registered domain of the form SLD.TLD where TLD is an existing ICANN approved TLD which TLD has a contract with ICANN (for example “.com”, “.org” or “.biz”). Any names not in the form KEY.sTLD, except certain reserved second level names for registry operations, will not be delegated without an approved change to this policy. The SO asks for complete authority over all DNS records placed in the sTLD zone including but not limited to A, PTR, MX, wildcard, and TXT and other records that are suitable for anti-spam or anti-forgery technology. A wildcard record may, for example, be inserted into the zone so that the SO can determine which unregistered domains are receiving lookup attempts (are being forged). A wildcard record will not be used to generate revenue or point to a public website.

Therefore, example policies/rules include:
1) Names registered in the TLD must be of the form key.sTLD, where key is of the form SLD.TLD where TLD is an ICANN TLD from the following list: com, net, org, info, biz, int, mil, gov, edu, and SLD is a domain name already registered in TLD.
2) The whois information at SLD.TLD is validated by various methods (details in other parts of this proposal)
3) The key domain must have been already registered for at least 6 months
4) All abuse messages for key.sTLD must be received by the SO
5) The website at key.sTLD will resolve to an SO-controlled web server and will display information regarding the registrant and the domain (details in other parts of this proposal)
6) When the registrant's email server (or an email server sending on behalf of the registrant) connects to the receiving email server, it must greet the receiving server with a HELO command of the format "HELO key.sTLD". The registrant must inform the SO of the IP's and hostnames of the sending mail server using the website at key.sTLD. The SO will enter A records in the DNS for the domain, for example "hostname.key.sTLD in A 123.123.123.123"
7) spam must not be sent from servers whose IP match the IPs for the A records in the key.sTLD name servers
8) registrants are encouraged to use sender authentication technologies such as SPF, Domain Keys, and Caller ID.

Authority is not sought in the following registry services areas:
1) In the aftermarket or with products such as WLS
2) Wildcard record that implements Sitefinder or something similar
3) Email products such as that offered by the .name registry
4) Auctions, Landrush or Sunrise. These are not necessary because only the registrant of the name in another ICANN TLD can get the name in this sTLD. This fact also eliminates trademark disputes in this sTLD.

Though a higher registration fee is designed to further the mission of the SO in reserving the namespace for non-spamming emailers, the SO requests authority to lower the per name registration fees, either the initial registration year fee, or follow-on registration years fee, if volume increase to the point were the RO, XO, SO, ICANN and other costs are covered while maintaining the stated mission.

The non-profit operation of the SO is, by its very nature, a structure which is likely a better guarantor of following stated policy than for-profit operations, because the profit motive is greatly diminished. The high per-name registration fee needed to register each domain is a guarantee that the SO will be both able to do its registrant verification procedures and remain a viable guarantor of the sTLD’s continued administration of the zone and perform the stated mission of this sTLD. Temptations to alter policy towards revenue generation at the expense of the Internet at large are minimal because of both the non-profit operation of the SO and a high per name fee factors. Also, after the normal initial registration 5-day grace period, the fee is non-refundable (because the fee is for validation and monitoring services, not for registration, which is free), therefore, there is no financial incentive or pressure on the SO to violate its own polices by putting unqualified domains in the zone.

The procedure that will allow the sponsored community to participate in policy formation is as follows: People who identify themselves as members of the community can participate in the SO-maintained forum on policy development. This forum facilitates a back-and-forth exchange of comments and ideas between the SO and the members of the community and between the members themselves. This forum will be monitored by the SO and the SO will post messages and encourage dialog there if necessary. Additionally, policy drafts will be posted to the SO website and to the forum where after a similar back-and-forth comment period on the SO policy forum, the SO board will take the information into consideration before taking a vote and enacting the policy.

The SO does not intend to vary from any existing ICANN policy. We observe that the SO's rules regarding valid whois may in fact enhance the enforcement of the current ICANN policies around whois information for certain names because each sTLD domain is tied to another domain in another ICANN TLD, so that when the domain's whois is validated, the whois for the name in the other TLD is validated as well.

Policy-Making Process

The policy making process will consist of the decisions made by the board members, including the decisions by the members regarding what processes the members wish to follow with respect to all or specific policy decisions. All decisions by the board shall be made based on a majority vote of a quorum of the board, except that a 2/3rd vote shall be required in the following instances: the election of new board members, the removal of existing board members, the addition or subtraction of board seats, or any change to the Articles of Incorporation or By-Laws which would result in a change in the voting control of any board member, or any determination by the board with respect to whether an individual board member has a conflict of interest with respect to a particular vote, such that such board member may not be allowed to vote on the matter in question. A quorum of the board is greater than half of the board members. There shall only be allowed to be an odd number of board members.

The board may delegate its authority to committees of the board, provided that no committee of the board may elect or remove board or committee members nor revise the Articles of Incorporation, the By-Laws, or the voting rules for a committee (though committees may make recommendations to the full board in regard to such matters). No committee may be constituted other than by act of the board. Committees are governed by the same voting rules which apply to the full board, except that committees may consist of an odd or an even number of members and that any tie vote on a committee will not constitute an affirmative vote by the committee. The term "meeting" used in this "Policy-Making Process" section refers to meetings of either the board or of a board committee and the term "members" refers to members of either the board or of a board committee, unless specifically stated otherwise.

The policy making process will take place at the regularly scheduled meetings and at such meetings as the members agree to hold from time to time. The members shall direct the maintenance of email fora or other similar communication system(s) which shall apprise the public of the schedule of meetings, the anticipated substance of the meetings, and the minutes of past meetings. The public shall be invited to use the communication system to provide input on the schedule and substance of meetings or on other matters that they believe of importance to the board. Special Advisors can also be called upon from time to time by the board to comment on policies and make recommendations in their areas of expertise. Any action may be proposed by any member and shall be considered by the other members if the proposed action is seconded by another member. Other than the regularly scheduled meetings which must be scheduled at a previous meeting (regularly scheduled or otherwise), meetings may only be called by a majority of members and shall be held after at least 10 days notice, unless 2/3rds or more of the members waive the notice requirement. As a result, action by the board or a committee may be considered at any time when at least one-half the members agree to call a meeting and when at least 2/3rds of the members agree to waive the notice requirement. Meetings may take place in person or through any media which allows an exchange of information among all the members in substantially real-time. Email shall not be considered "real-time," though chat shall be. The minutes of all meetings shall be recorded and made available through the public fora no later than 10 days after the meeting.

A. Add new value to the Internet name space

Use of the sTLD will not eliminate spam across the Internet. Spam will still be sent using other TLDs and there are many efforts to reduce spam. The SO can guarantee that message sent using names in the sTLD will be very nearly spam-free. Usage of the sTLD can dramatically increase the number of non-spam messages that get through to their destination, and indirectly reduce the number of spoofed senders (messages that say they come from a domain but actually, do not), and make spam messages sent using other TLDs more easily identifiable, then that is of significant value to the Internet at large.

What is the value of increasing the likelihood of your message actually reaching its destination? Whatever value that is, and the SO believes it to be significant, that is the value that will be added to the namespace for each message sent that utilizes each name registered.

Name value: The sTLD string
Though the core community the sTLD is aimed at is the group of technical mail server operators (both the senders and the receivers), the broader Internet community benefits because that wider community sends and receives email. The only part of the Internet community that will not benefit are the people who send email but do not send it according to the policies of this sTLD, and even those people are not prohibited from sending mail. They are still able to send it, they just cannot use the sTLD to help the mail reach its destination. We would like the sTLD string to be as generic as possible because then the wider community of Internet users have an easy, and more important, memorable, way to 1) visit the site of the mail sender with verified information regarding the sender displayed there, and 2) to complain about sent mail by submitting an abuse complaint. Just add ".mail" to the domain to send an abuse or to see information about the sender.

Additionally it adds value to the other parts of the name space because the whois information for the other TLDs would be validated for some portion of those names that are also registered in this sTLD. Also, if adoption becomes widespread, because the other registries' would need a contract with ICANN in order for its TLD to be used as second-level-domain in this sTLD, it provides a slight incentive/benefit for the ones that do not have a contract to make a contract with ICANN.

Enhanced diversity of the Internet name space
Due to its uniqueness, this sTLD adds to the diversity of the Internet name

space. It expands the number of dimensions for which a domain name can be used. In this case, the name both represents a validated identification and also an underlying system that enriches one of the most basic functionalities of the Internet: email. The sTLD provides an additional "layer" to other parts of the namespace increasing their utility by allowing them to participate in a responsible email community.

Since the registration of a domain in the sTLD is based upon the prior existence of the key domain, only the registered user of the key domain may register the sTLD domain. What this means is that any registered name in the sTLD will, by definition, be put into active use, and will remain as long as the registrant follows the policies. Furthermore, this ensures that there is very little chance that a domain in the sTLD may be cybersquated hijacked or defensively registered. This also means that there will not be, indeed, cannot be any land rush or sunrise headaches.

Part of this sTLD's mission is to distinguish one group of users from another group. A TLD is intended to be an easily remembered, clear, logical, classification of a community of Internet users not already classified. It makes them easily identifiable by other users. By using a second level domain, this community of users would be mixed-in with the other TLD's users, and this clarity is lost.

The SO realizes that the risks of not using a TLD are severe. If, for whatever reason, there was a service interruption in the delegation of the SLD, the entire, now established, trust system would be neutralized.
* There is a risk that the TLD in which the SLD was registered, goes under.
* The second-level-name we select is revoked. Many if not all registration contracts reserve the right of the registry to remove the name for any reason.
* A legal proceeding could be filed against the registry compelling them to suspend the domain at best and delete it at worst, this could be something as simple as a UDRP proceeding. The SO, being delegated a sTLD, would be in complete control in all these circumstances and would not have to rely on another party for security.

To illustrate, with an SLD, were it to be taken out of the TLD zone for any reason, validation queries (by the receiving mail server) will return NXDOMAIN, the DNS response for “domain not found.” In this case the receiving mail server is instructed to distrust the source of mail. This is the response we will send when the mail source is, in fact, not trusted. Therefore, the effect of being removed from the TLD zone would be that all trust verifications would actively fail. If this were to happen, all receiving mail servers that were using the SLD would break and they would have to change their code. A failure of the DNS itself results in a time-out, which is not an active failure, and in this case the receiving mail server is instructed to fall back on alternative methods of verification. With a TLD, as we would not take ourselves out of the root zone for any reason, an NXDOMAIN would not be generated falsely.

Also, it is desirable for the string to be an easy memorable mnemonic because the public, if it remembers the sting, can use it to easily find information on the mail sender or to easily send abuse messages to the SO by simply appending the string to the end of the key domain. With a second-level name this benefit is greatly reduced.

Reach and enrich broad global communities
Internet users who have not registered names in the sTLD benefit from the sTLD

because their receiving mail servers can more easily distinguish messages that are not spam. Also, as adoption increases, the price can decrease, so that not only are more and more receivers able to partake in the benefits of spam-free email from more people using the domains in the sTLD, but also more and more senders, are able to get their non-spam messages through.

B. Protect the rights of others

Any domain name registered in the sTLD must first be registered in another TLD, the rights and obligations of every other TLD are reflected and made more secure. Information producers and consumers will be able to interact with greater confidence, free(er) from trespass and with the basic knowledge that a registrant has a verified mailing address. The rights of everyone in all TLDs will be enhanced. In terms of compliance with ICANN policies designed to protect the rights of others, the sTLD will add to WHOIS compliance across all TLDs. While this sTLD, by itself, will not end all illegal and abusive email practices on the Internet, it adds to the ways such practices can be avoided. WHOIS policies inevitably attempt to balance competing interests such as reliable identification versus free speech and anonymity, while also creating the potential for misuse of WHOIS information itself. This sTLD adds to the diversity of ways to balance these dilemmas and creates a new incentive for compliance: more reliable email communication. This sTLD risks no derogation of the rights of others and only furthers reliable self-identification and communication among all interests, groups and constituencies, proprietary or otherwise.

In addition, spam, much like a telemarketing phone call, can be considered an invasion of ones privacy rights, one of the purposes of the sTLD is to help protect the rights of people to receive spam-free email.

C. Assurance of charter-compliant registrations and avoidance of abusive registration practices

Registered names in the sTLD are of the form "key.sTLD" where "key" is a domain name that is already registered in another TLD. The list of applicable TLDs is constrained to TLD registries that either have contract with ICANN and comply with the UDRP and other ICANN policies or are ".mil", ".edu", ".gov", ".int" which are restricted TLDs.

There are three basic elements of a charter-compliant registration in this sTLD: 1) Registration and listing of one's WHOIS information in the Key Domain in another TLD; 2) No spam; and 3) Confirmed WHOIS. The registration and WHOIS listing of the Key Domain and the spam policies of this sTLD are discussed elsewhere in this application. WHOIS compliance will be verified by requiring the mailing of all application materials and the matching of WHOIS with the correspondence address. Existing WHOIS information will be verified at the following times: on any change in the Key Domain's WHOIS information, upon the lodging of a substantiated ("Substantiated" means that the WHOIS information itself is patently false or incomplete based on addressing standards for the claimed jurisdiction or that the WHOIS is demonstrated to be false through the presentation of evidence of mail returned "undeliverable" or "addressee unknown," or similar.) allegation of false WHOIS, and otherwise a minimum of once a year or as otherwise directed by ICANN's WHOIS policies. At least one contact each will be attempted via email, telephone, and facsimile and two attempts at contact via mail will be attempted before a name is de-listed from the zone one month after the first attempted contact. A successful non-mail contact in the last week of the month will give the registrant one additional week to succeed in achieving a mail contact. The sTLD will not be an additional forum for hearing disputes regarding the registration of domain names in other TLDs -- each TLD will rightly retain its own jurisdiction over its own policies. Significantly, the sTLD creates a new incentive -- more confident communication -- for compliance with WHOIS, UDRP, every other policy or law the violation of which results in a change in a domain name's WHOIS information.

IP Rights

Registrations that infringe on the intellectual property rights of others will not only be discouraged, they will be not allowed, because only the registrant of the key domain will be allowed to register that domain in the sTLD. If there is an intellectual property dispute with the key domain, the new registrant of the key domain is also the new registrant of the sTLD domain. We do not expect there will be a trademark dispute over, for example "example.com.mail", and not over "example.com".

Charter-compliant persons or entities that are allowed to register names:

This is nearly the entire purpose of the SO: to determine which registrants (and their domains) are members of the community who follow the policies and send spam-free email. It is part of the registration process that determines if the key domain is compliant with the policies and also, once in the sTLD zone, that the key domain and email sent using the sTLD continues to comply.

Reservation list

All the names in the entire namespace are reserved because, all the names on the second level are reserved for future use. Only those strings that match stings of approved TLDs, will be utilized on the second level. All the names on the third level are reserved for use by the second-level registrant at another TLD registry.

Minimize abusive registrations

Abusive registrations will be minimized for two reasons:
1) The high per name-year fee
2) The key domain must already be registered in the key domain TLD for at least 6 months.
Additionally, all abuse messages for each domain will be received by the SO, not by the registrant. These messages will be used to determine if the registrant's registration is abusive, and if it is, it will be removed from the zone by the SO.
There will be no "rush" on the names when the registry opens based on the trademark or other value of the name itself because only the registrant of the key domain will be the registrant of the key.sTLD domain

Comply with trademark and anti-cyber squatting legislation

The SO expects to fully comply with whatever applicable trademark and anti-cyber squatting legislation that might exist or be enacted during the course of our sTLD administration.

Provide protections for famous names and trademarks

Famous names and trademarks are protected because no name will be registered in the sTLD that has not already been registered in the key domain TLD. The disputes regarding names in the other TLD have very likely already been settled because the key name must have been registered for at least six months there. Nevertheless, if there are any disputes, the SO and the registrars making registrations will agree to abide by any UDRP or other (court-order) dispute resolution mechanism. No disputes are anticipated. Also, there is no need for a sunrise period in which to provide these protections because only the registrant of the key name may obtain the key.sTLD domain name.

D. Assurance of adequate dispute-resolution mechanisms

Because a Key Domain is a pre-requisite to listing a domain name in the zone of this sTLD, UDRP, start-up (sunrise), and similar dispute resolution procedures are not required, though if a UDRP is brought it will be complied with. Dispute resolution mechanisms relating to WHOIS and spam are covered elsewhere in this application.

E. Provision of ICANN-policy compliant WHOIS service

The whois information is integral to the operation of this sTLD because even with technologies that prevent sender spoofing (Sender Authentication Technologies that prevent forged "from" and other addresses), the registrant can still spam, and if the whois information is not validated or checked at all, then it is very difficult to find out who, really, is behind it.

Part of the per-name-year fee is to be used to perform various validity checks on the whois information of the underlying ("key" domain, as we call it) domain name. Also, a requirement is that this key domain must be registered for at least 6 months before the sTLD domain will be placed in the zone. Validity checks include 1) sending postal mail using either a governmental postal system or courier such FedEx to the registrant or administrative contact and providing a system whereby the registrant can confirm receipt of the postal mail and 2) Sending email to verify that the email address in the whois works and that mail sent to that address is received by the registrant. The SO reserves the right to also perform other whois information verifications such as calling the phone number listed in the whois, sending faxes to the fax number, contacting the other whois contacts such as the technical contact, as well as on-site in-person visits to the location listed in the whois, and other investigations.

Due to the fact that many large companies and other members of the Sponsored Community list only their corporate address in the whois for the key domain, two optional fields can be entered when registering sTLD names. These will be communicated by the registrars to the registry using the EPP protocol. These fields are a "Care Of" name, which is the name of a contact person at the address where the postal mail will be sent, and an "Alternative Email" address, which email address must be in the key domain. If these optional fields are used by the registrant, postal mail will be sent to the address listed in the whois with "Care of" line as the person's name, and mail sent to the optional email address will also be sent to the email address listed in the whois output. Registrants will not be transmitting the whois to the sTLD operator (the RO) via the registrars. This information will be provided to the RO by the XO who will use the zone file generated by the RO to determine those key domains for which to obtain whois information at the other TLDs. This information will then be transmitted from the XO to the RO for insertion into the RO's ICANN compliant whois database, and as the current whois policy states, is accessible to the public. The XO will monitor the zone files and the whois of the other TLDs daily so that any modifications made there will be transmitted and noted, with little delay, by the RO (one of the policies by the SO is that if the key domain is removed from the zone of the other TLD it is also removed from the zone of the sTLD). If the whois information on the key domain changes, then the SO reserves the right to re-validate the new whois information at no charge to the registrant, and it would if the changes were significant. If the whois information was seen to be changing often, the sTLD domain may be removed from the zone.

The registrant agrees to allow the whois information that was validated to appear at the website "example.com.mail" (in a graphical format) which is maintained by the XO for the RO. This allows the members of the community the opportunity to see the most recently validated whois information for each domain by simply using a browser and adding ".mail" to the end of the domain name in question.

The method described will be modified, if necessary, by changes in ICANN's whois policy, as well as any changes that would need to be made to the output of the whois database (port-43 or otherwise) by the RO, if those are required by changes in ICANN's whois policies.