

2011/06/10
第1回DRP検討委員会
資料9

CONCEPT PAPER

gTLD ZONE FILE ACCESS IN THE PRESENCE OF LARGE NUMBERS OF TLDS

STATUS OF THIS DOCUMENT

This is the Current Draft of the Zone File Access Concept Paper as developed by the community led Zone File Access Advisory Group. A final version of this Concept Paper is intended to be posted for public comment by the ICANN community and also presented for discussion at the ICANN meetings in Nairobi Kenya.

SUMMARY

This report is submitted to the ICANN community for comment as part of the ongoing work in developing the Applicant Guidebook for new gTLDs.

Contents

1.0	EXECUTIVE SUMMARY	3
2.0	PROBLEM STATEMENT.....	5
3.0	SOLUTION SPACE AND REQUIREMENTS	5
4.0	BACKGROUND.....	5
5.0	ISSUES IN THE CURRENT SYSTEM.....	7
5.1	Zone File Access Requirements for Providers.....	8
5.2	Zone File Access Experience Among Providers.....	8
5.3	Zone File Access Requirements for Consumers.....	9
5.4	Zone File Access Experience Among Consumers.....	9
5.5	Zone File Access Operational Issues	10
6.0	IMPLICATIONS OF gTLD EXPANSION ON ZONE FILE ACCESS	11
7.0	ALTERNATIVE MODELS FOR gTLD ZONE FILE ACCESS.....	12
7.1	Understanding the Four Alternative Models.....	12
7.1.1	The Enhanced Bi-lateral Model.....	13
7.1.2	Third Party Approaches (Repository, Proxy and Clearinghouse).....	14
7.1.3	Registry operations/relationships with the ZFAPP – Repository and Proxy Models	15
7.1.4	Consumer operations /relationships with a ZFAPP -- Repository and Proxy Models.....	15
7.2	ZFA Model Comparison.....	17
7.3	Four ZFA Models: Advantages and Disadvantages	19
7.4	Cost Models for Alternative Zone File Access Strategies.....	20
7.5	Funding Models for gTLD Zone File Access.....	20
7.5.1	Funding Scenarios for ZFA Consumers.....	20
7.5.2	Funding Scenarios for ZFA Providers.....	21
7.5.3	ZFAPP Operational Model	21
7.6	Issues Addressed in a Third Party ZFA System.....	22
7.6.1	gTLD Operator Benefits.....	22
7.6.2	Zone File Consumer Benefits	22
8.0	NO EFFECT ON ENHANCED REGISTRY SERVICES.....	23
9.0	POTENTIAL FOR ENHANCED DATA SERVICES.....	23
	ANNEX A – PARTICIPANTS IN THE ZONE FILE ACCESS ADVISORY GROUP	25
	ANNEX B – TYPICAL ZONE FILE ACCESS AGREEMENT	26

1.0 EXECUTIVE SUMMARY

The root zone of the DNS currently contains 279 top-level domains (TLDs). Of these, sixteen are generic top-level domains (gTLDs) and there will be a seventeenth once .POST has been delegated. The registries that run these gTLDs maintain DNS zone files that contain resource records for the domain names that are active within those gTLDs. The registries also operate the authoritative name servers for the TLD zone. TLD name servers most frequently resolve name server DNS names of domains registered in the TLD zone to IP addresses. For the purposes of this Concept Paper, the collection of these records is called a Zone File.

Prior to the existence of ICANN, Zone Files were available to researchers, brand owners and others for business purposes from gTLD registries. Today, the ICANN gTLD Registry Agreement requires that a gTLD registry provide access to Zone Files to any person or organization that signs and abides by a Zone File Access (ZFA) Agreement. Contracted gTLD registries provide this access daily and at no charge. The relationship between the gTLD registry and the organization requesting Zone File Access is established and maintained by the registry and a zone file consumer: no third-party mediates between the two. This means that each gTLD registry has direct knowledge and control over the relationships between itself and those consumers have entered into an agreement to access the Zone File.

gTLD registries differ in the manner in which they authorize and provide Zone File Access. Zone file consumers deal with these differences today on a case-by-case basis and this solution works reasonably well given the relatively small number of Zone Files.

This leads to a natural question: *is the current manner of providing Zone File Access sufficient in an environment where there may be a dramatic increase in the number of gTLDs?*

If the top level of the domain name system expands to hundreds – or even thousands – of new gTLDs, the current bi-lateral contractual and access arrangements for ZFA providers and consumers will neither be efficient nor scale effectively for zone file consumers.

This leads to a second question: *are there models for a new approach to Zone File Access that would ensure continued, consistent access for consumers of the data while preserving registries right to monitor and, where necessary, control that access?*

In December of 2009, ICANN established a Zone File Access Advisory Group to examine this question and to study whether there were models that could meet these requirements. This Concept Paper is the initial result of that Advisory Group's discussions.

The Advisory Group identified several approaches that could reshape Zone File Access so that it meets the needs of both providers and consumers of the zone file data in an environment where the gTLD space is dramatically expanded. This Concept Paper considers issues that exist with TLD zone access today, examines the current set of constraints and limitations, discusses why the current system

scales poorly as the number of registries increases, and proposes alternative models for TLD zone file access. Specifically, this Concept Paper provides a careful look at four models for Zone File Access in an environment with many new gTLDs. Three of these models have one thing in common: the introduction of an independent third-party between the providers and consumers of the Zone File information. The goal of introducing this intermediary is to provide a scalable and consistent approach for authorization and distribution of the data. The models differ distinctly in the role of that third-party. None of the models impose any limitation on a gTLD registry's ability to monitor and control access or provide value-added services that go beyond simple access to the zone file.

The four models each have distinct advantages and disadvantages and a detailed description for each is provided later in this document. In summary, the four models are:

- An **enhanced bi-lateral model** where the essential elements of relationships between registries and consumers become standardized;
- A **repository model** where a third-party collects zone files from registries and distributes them to zone file consumers;
- A **proxy model** where a third-party acts as an intermediary for standardized authorization and where data is delivered via secure proxy connections to the registry; and,
- A **clearinghouse model** where credentials and authorization are maintained by an intermediary but where data is delivered over secure connections between the consumer and the registry.

In its work, the Advisory Group has also done preliminary work on identifying how funding for a third party Zone File Access Program Provider would be established. There has also been a discussion of models for allocations of transactional costs associated with Zone File access. In this Concept Paper these issues remain at a preliminary stage and need further community discussion.

During its discussions, and during the development of this Concept Paper, the ZFA Advisory Group questioned whether its work and any of its recommendations might have policy implications that should be considered by the GNSO. The Advisory Group will engage the GNSO on this issue as part of the public comment process on the Concept Paper. The ZFA Advisory Group invites broad public discussion of the problem space and potential models for meeting the needs of the Zone File Access provider and consumer communities.

2.0 PROBLEM STATEMENT

The current model for Zone File Access is built on individual, bi-lateral agreements and operational relationships between consumers and providers of data. Scaling this model into an environment where there are many consumers and providers may create both operational and cost problems for both consumers and providers of data. A new model for Zone File Access that can scale in both the current environment, and in an environment including new TLDs, may be needed to address these concerns.

3.0 SOLUTION SPACE AND REQUIREMENTS

Solutions for multilateral, scalable, secure and consistent Zone File Access may be implemented as a complementary solution to the existing bilateral approach. Any solution must recognize that the record types or data contained in the zone files may vary in new, emerging registry models.

Additionally, improving the current model will also provide opportunities for operational and cost improvements for producers of data. Any new model for Zone File Access must be resilient and defend against abuse through both administrative and technological means, and should preserve or enhance existing models of access for legacy consumers. Access to Zone Data should be granted on an equal, non-discriminatory basis among qualified Consumers. Nothing in a new model for Zone File Access should limit any registries' ability to innovate or provide new products and services.

4.0 BACKGROUND

gTLD zone files contain all domain names currently active within a given TLD and the hostnames of authoritative name servers for each domain name. The gTLD zone file also contains glue records that map name server hostnames to specific IP addresses. Many other DNS resource records may be present (e.g. DNSSEC, NAPTR, TXT and others).

Currently gTLD registries are required by ICANN agreements to provide access to a copy of their TLD zone files to any entity that signs an access agreement and thus agrees to adhere to the registry's terms of service. Registries must provide zone file access at no charge, on at least a daily basis. TLD zone file consumers range from academic researchers and law enforcement to security companies and intellectual property protection firms -- amongst others. Each entity that desires access must sign a zone file access agreement with each registry from which they wish to obtain zone files. Hundreds of entities have created processes or automation to download these zone files in order to obtain data on the current set of domains registered in various gTLD zones. The following table gives a view of the total number of "accounts" at each of the existing gTLD zones as of September 2009. [see table, next page]

gTLD	Total Number Of ZFA Accounts	Recent Monthly Change
.com/.net	828	+ 33
.biz	703	+ 3
.org	691	+ 6
.info	426	+ 5
.name	203	+ 8
.mobi	185	+ 1
.asia	73	+ 1
.aero	42	Unchanged
.pro	53	+ 1
.coop	33	Unchanged
.tel	32	+ 3
.travel	26	Unchanged
.cat	11	Unknown
.museum	Unknown	Unknown
.jobs	Unknown	Unknown

Access to TLD zone data is typically provided via a password protected, unencrypted FTP server. Measures to protect FTP servers from unauthorized access vary across registries. The amount of zone data transferred during a single access varies across registries: smaller zone files only take up a few hundred kilobytes of data, while the largest (i.e. .com) zone is many gigabytes (compressed), and can take hours to download.

Historically, in an environment where there were few gTLDs, zone files were provided on an as requested, as needed basis. This arrangement was maintained when ICANN negotiated its initial registry agreements. The current registry agreement provides, generally in Appendix 3, the mechanism that has evolved to support Zone File Access (a typical example of the Zone File Access Agreement is presented in ANNEX B).

In contrast, ccTLDs do not, in general, provide Zone File access. Some of the European ccTLDs that were providing some level of access ended their provision of access circa 2003. The reason generally given was that the data was being abused. Some of the abuse was indirect use of the zone file to support mining whois data to try to get a registrant to transfer their domain to a new registrar or host -- sometimes at a higher fee. One of the other reasons access was denied was due to directory scams where registrants would be sent what was a disguised invoice for inclusion in a directory. In this exploit it is believed that some of the registrant data was mined from WHOIS data. The cost of inclusion was often around \$1000 per year. The registrant would, thinking that it was some kind of official and free inclusion directory, send back the signed document and would then be pursued for the inclusion fee. Some of these directory scammers go as far as to set up directories (see <http://www.scamwatch.gov.au/content/index.phtml/tag/DirectoriesAndAdvertisingFalseBilling#h210> for an example). Another reason that many ccTLD registries don't provide zone file access is that it may

contravene national Data Protection/Privacy legislation. It is not clear whether this has ever been tested in any relevant national legal system.

Today, consumers of TLD zone data have only a few zone files to download. Each consumer of TLD zone data must apply for and be granted zone file access with each gTLD registry operator. Upon receiving approval, the consumer must put in place an operational procedure to access to each zone file, according to the policies and technology adopted by each TLD registry operator. The contracts, acceptable use policies, and operational procedures have not, over the years, changed a great deal. Some registry operators run multiple gTLD registries and/or provide back-end data technical services for multiple registries. Such registries typically continue to provide zone file access for each gTLD on separate infrastructure however, and under different terms.

For each zone file access arrangement, the consumer and registry must exchange security (e.g. access controls such as the customer's IP address) and account information (e.g. authentication information) prior to access. Both parties must maintain this information over time. While the current arrangements are adequate for small numbers of registries (n) and modest numbers of data consumers (m), they become increasingly problematic and costly should either or both (n) and (m) grow. In particular, the creation of IDNs and new TLDs has the potential to increase (n) by a factor of 10, 100, or more. Moreover, the inclusion of DNSSEC and digitally signed data in TLD zone files will increase the sizes of zone files. The increase in the size of the zone files require increases in infrastructure spending to avoid latency issues for TLD zone data consumers and bandwidth/capacity issues for registry operators.

5.0 ISSUES IN THE CURRENT SYSTEM

The current zone file access system works, but there are some shortcomings in its current state.

Consumers of zone file data face costs and responsibilities that could be significantly reduced through a more efficient system. The need to create separate processes for accessing each zone, and use different credentials for each zone file access agreement introduces inefficiencies, uncertainties and avoidable costs. Registries provide different access methods and Acceptable Use Policies (AUPs), meaning that consumers have to manage disparate processes and segregate data differently, depending on the TLD. Further, since disparate access systems are used, processes or automation implemented by zone file consumers are more prone to break. When errors result in loss of access, problem resolution is cumbersome for data consumers, since the consumer must engage with unique reporting systems to resolve the problem. For example, a change in zone file consumer's infrastructure (e.g. firewalls, IP delegation, systems libraries) may affect zone data retrieval operations for certain registries but not others. Slow downloads from one registry could affect how a consumer's automation manages other scheduled downloads. Lastly, consumers must manage change: when a registry introduces a change in its access method system or data path, the consumer must accommodate these changes in its own systems. Often, a data consumer's automation consolidates zone file data collected from many registries. Thus, any change has broader impact and so a larger matrix of testing is required every time a data consumer needs to update its own systems.

In general, providing reliable access to zone file data imposes operational costs and liabilities on the gTLD registries without direct compensation. While this has been accepted by registry operators as a cost associated with operating one of the Internet's primary namespaces, it would be logical for registries to lower these costs if there were more efficient ways to provide this access. For example, registries are required to provide continuous access to all takers, without any specific Service Level Agreements (SLA's) specified. This clearly costs money to operate. The registry is also responsible for providing a secure connection and clean data file to data consumers, which creates significant security requirements for registries.

5.1 Zone File Access Requirements for Providers

The burdens for gTLD registries appear to include, at least, the following:

- 1) Create and maintain zone file access legal agreement (if the agreements were standardized this may not be a requirement)
- 2) Provide method for data consumers to apply for access
- 3) Receive, review, and countersign all agreements
- 4) Provide initial access credentials to data correspondents
- 5) Create and maintain access credentials for all data consumers
- 6) Securely archive all legal agreements
- 7) Send updates to access agreement to all data consumers
- 8) Maintain redundant, high-availability FTP servers for access to zone files
- 9) Maintain high-bandwidth, redundant access connectivity to FTP servers
- 10) Provide timely updates and full change management to all data consumers for any changes in access arrangements, security measures, or other operating procedures
- 11) Maintain security for FTP servers
- 12) Update FTP server from main zone file database
- 13) Ensure the integrity of the zone file copy on the publication server
- 14) Provide methodology for data consumers to recover or update access credentials and contact information
- 15) Field support questions and issues with access problems
- 16) Watch for suspicious behavior to prevent system abuse
- 17) Take enforcement actions, including agreement termination, in proven cases

5.2 Zone File Access Experience Among Providers

Zone File Access providers tend to have a set of initial costs associated with setting up Zone File Access for consumers of the data. However, once the initial task of setting up the system is in place, the costs for data subscribers is linear in respect to the number of accounts granted access. Anecdotal evidence suggests that once the access is established, the ongoing operational cost is marginal compared to the other activities of the provider. As an example, the bandwidth to transfer a daily copy of a very large zone would be substantial. However, when compared to bandwidth requirements for other activities of registries that administer very large zones, Zone File Access data provisioning may be a nominal cost.

Anecdotal evidence, provided by several registries, also suggests that the administrative cost to providers is relatively low. One reason for this is that there is no significant churn in the accounts that have access to Zone File data. In fact, research conducted so far indicates an approach where, once the accounts are set up, they are largely allowed to function without significant ongoing monitoring or auditing. This does not change the requirement that the ability to monitor, audit or control should be in place.

5.3 Zone File Access Requirements for Consumers

As consumers, we believe these burdens may become unmanageable if growth in the numbers of IDN TLDs and new gTLDs occurs as speculated:

- 1) Obtain zone file agreements for all gTLD registries
- 2) Have legal counsel review each agreement (if the agreements were standardized this may not be a requirement)
- 3) Securely archive all legal agreements
- 4) Create separate process to access each zone file regularly
- 5) Maintain security for FTP server connections
- 6) Maintain security of accessing server and local copies of zone files
- 7) Obtain access credentials for all gTLD registries
- 8) Securely store and manage all access credentials
- 9) Request updates to access credentials from all gTLD operators using restricted IP access whenever infrastructure changes require movement of accessing server
- 10) Download each zone file on a daily, scheduled basis
- 11) Ensure the complete transmission of zone file data
- 12) Test the accuracy/integrity of downloaded zone files
- 13) Aggregate and normalize zone data for use by consumer's application/automation
Report any problems with a zone file to the appropriate registry, following -- up if there is no response or an inaccurate one.

5.4 Zone File Access Experience Among Consumers

Typically, consumers find the application process for Zone File Access to be reasonably simple. The key reason for this is that the zone file access agreement is part of the existing registry agreement and is common to all registries. Effectively, the consumer agrees to a standard of conduct and the Zone File provider will agree to provide credentials for the service.

Several zone file consumers have reported that it is sometimes not obvious where requests for Zone File access should be submitted. Responsiveness among the providers is reported to be generally good with a few exceptions.

For most zone file consumers the challenge begins after the administrative process is completed. The access methods for zone file data vary from registry to registry. Examples of access strategies include:

- FTP Servers;
- Password protected web sites; and,
- AXFR access to a name server

Methods vary even within these three strategies; for example, in the case of FTP servers, consumers have found that how zone data is organized and whether they are compressed or encrypted varies from registry to registry.

5.5 Zone File Access Operational Issues

Beyond the individual challenges and experiences listed above, there are several issues that arise in the practical application of current zone file access for daily operations:

- 1) Risk of unauthorized access is higher than desirable.
 - a. Zone data and access credentials may be transmitted in the clear – encryption via secure FTP, IPsec encryption or SSL connections is not common.
 - b. In most cases, password management is neither enabled on server platforms (e.g. aging out old passwords regularly, requiring strong passwords)
 - c. Monitoring of access to detect abuse is not uniform. Zone file consumers among the ZFA Advisory Group observe that it is possible to perform multiple downloads daily from certain registries.
 - d. Some registries use source IP verification to identify zone file consumers. The public IP space used by many zone file consumers is readily obtainable and IP spoofing is trivially easy to perform.
 - e. Certain registries do not restrict FTP access to specific source IP addresses at all, but rely on authentication alone to protect access to their zone file systems (i.e. FTP username/password logins only with no other measures for verification of identity).
 - f. Other security measures – DDoS protection, protection against protocol specific attacks, traffic and log analysis – are not uniformly present across all registries.
- 2) Costs are significant for a non-essential, uncompensated registry function.
 - a. Registries must provide zone file access for free, yet the systems and network infrastructure to properly provide this service are non-trivial. This is especially the case for the largest registries.
 - b. Customer care and problem resolution are recurring costs for registries. Breakdowns of the individual transmission systems and corruptions of FTP files are not uncommon. Further, no standard/metrics for availability or performance are specified, which leads to disparities in up time, mean times to restore, etc. and expectations around those activities. While the service is free, zone file consumers are dependent on the availability of the data. Thus, when issues inevitably arise, complaints from zone file consumers will impact customer service operations of a registry in unpredictable ways, and in some cases, significantly.
- 3) Infrastructure change management is difficult for both parties.

- a. Access requirements and IP restrictions to download data are not uniform. Security measures vary. Some registries restrict IPs and monitor login attempts closely. Others employ different measures. Consumers must account for each nuance in security measures and be able to respond quickly to policy changes a registry may introduce to ensure access is not lost. Similarly, registries must provide timely updates and full change management to all data consumers for any changes in access arrangement, security measures, or other operating procedures.
 - b. Any change in the consumer's network infrastructure that affects zone file access, i.e., a renumbering of the IP addresses of the consumer's hosts that access zone files, requires an update to be sent to all gTLDs that restrict access by IP address. These changes have to be managed across all processes pulling zone files carefully to ensure access is not lost.
 - c. gTLD registries must notify hundreds of consumers any time they need to make changes to IP addresses or other access procedures. From the purview of consumers, this seems to be such a serious burden that certain registries have avoided upgrading infrastructure to support improvements and efficiencies. This is most apparent in the non-migration of obtained registries by the receiving registries to a common platform for zone updates.
- 4) No standards or metrics for availability or performance are specified in registry agreements. ZFA Advisory Group members indicate that they observe disparities in availability, mean times to restore, mean time between service outages, etc. Registries have different expectations regarding their responsibilities with respect to these measures of service level and performance.

6.0 IMPLICATIONS OF gTLD EXPANSION ON ZONE FILE ACCESS

Currently ICANN is in the process of opening up a much larger namespace to a wider variety of registry operators. Estimates of new gTLD's typically predict several hundred new "dots". The addition of hundreds of new registries with a wide variety of business models creates numerous scaling issues and costs for data consumers.

- 1) Potentially hundreds of contracts to review, sign, and securely archive.
- 2) Potentially hundreds of new data retrieval processes to create and maintain – accessing hundreds of files around the Internet.
- 3) Increasingly complex systems needed to manage the dispersed data sources and access capabilities and respond to the inevitable increase in break-downs disparate data systems will have.
- 4) More complex problem resolution processes to manage the trouble resolution across the larger number of zone file access providers.
- 5) Change management will be a highly intensive operation – requiring creating and managing hundreds of requests.
- 6) A preliminary cost model developed by the Advisory Group shows that costs to create and maintain the systems necessary to get full coverage of gTLD zones could increase from thousands of dollars to 2 orders of magnitude higher.

Each new gTLD operator will have to go through considerable expense to set-up their own capabilities, legal, operational, and systems, in order to support the same infrastructures already in-place for existing gTLDs. In order to properly maintain all the requirements to support the new zone file users, costs could be considerable for a new registry. Absent any standards or conventions or common supplies (outsourcing agent), some new gTLD operators will emulate existing gTLD practices but other will likely set their own, resulting in even more diversity for zone file consumers to accommodate.

Existing gTLD operators may have to expand their infrastructure to accommodate more data (resulting from the adoption of DNSSEC) and additional zone file consumers (it is only reasonable to assume that expansion of the TLD name space will attract more research, speculation, analysis, and security services as well as more interest from governments and law enforcement). If outsourced to an existing provider, some significant cost savings could be realized by re-utilizing standing systems. However this strategy hasn't been seen in prior gTLD expansions or consolidations, as separate infrastructures and legal agreements are typically maintained. Further, for such operators, there are still unavoidable costs and complexities needed to support differing access levels, as zone file access customer bases are not identical across gTLDs.

The Zone File Access Advisory Group believes that new models for ZFA should be explored. Such models should ensure continued, consistent access for consumers of the data while preserving registries' right to monitor and, where necessary, control that access. Moreover, the new models should seek to remain as close as possible to the current costs of access for consumers and costs of service to the providers.

7.0 ALTERNATIVE MODELS FOR gTLD ZONE FILE ACCESS

Four alternative models for gTLD Zone File access are presented. The goal is to find a solution that meets both provider and consumer requirements in an environment where the number of gTLDs is significantly expanded. Briefly, the four alternative models are:

- Enhanced Bi-lateral model;
- Repository model;
- Proxy model; and,
- Clearinghouse model.

7.1 Understanding the Four Alternative Models

During the course of its work, the Advisory Group identified two approaches to enhancing Zone File access: 1) improve the existing Bi-lateral arrangement so that it more effectively meets the needs of consumers and providers while scaling adequately to meet the demands of a large number of new gTLDs; or, 2) using a third party to facilitate the interactions between consumers and providers.

7.1.1 The Enhanced Bi-lateral Model

The intent of the Enhanced Bi-lateral model is to take the approach of the existing system of bi-lateral registry-consumer agreements and evolve it addressing its main drawbacks such as inconsistency and inefficiency of subscription and data delivery methods.

Existing gTLD registries are already using identical zone file access agreements; however the process of entering into such agreement, content delivery protocol, frequency of data updates and methods of customer support currently varies from registry to registry.

In the Enhanced Bi-lateral model it is suggested that the essential elements of relationships between registries and consumers become standardized. This can help mitigate scaling problems. For professional data consumers addition of new registries as data suppliers will only involve invocation of well documented and easily programmable procedures.

The following processes and protocols can be part of the standardization effort:

- process of applying for zone file access
- submission of zone file access agreement
- data transmission protocol
- path and naming conventions for the zone file
- timing of zone file updates
- procedures for customer support
- security-related procedures (such as changing access passwords)
- change management procedures (such as registry moving the file server to a new address)

Besides, certain technical inefficiencies may also be addressed within the framework of existing bi-lateral system. A variety of new technologies for data access and delivery have emerged over the last years. These technologies may provide more efficient and secure methods for user authentication, managing access credentials and data delivery.

During the work of the Advisory Group there were preliminary discussions concerning certain technical solutions that can possibly be used to improve zone file access procedures, however more expert analysis is required in this direction to examine the suitability of specific technologies.

Solutions suggested in this chapter can also be applied in combination with other improvements of the zone file access system such as the Clearinghouse model described below.

7.1.2 Third Party Approaches (Repository, Proxy and Clearinghouse)

Another possible solution is a single platform for all zone file transfer management combined with a managed access agreement structure. In this plan, a designated, vetted, and trusted third party operator would handle all aspects of TLD zone file access, from enrollment to standard operations and updates. As a result, the current requirement imposed on gTLD registries to provide free access to individual data consumers may be removed. Such an entity could reduce operational cost and burdens pointed out above for gTLD operators, while dramatically improving the picture facing data consumers staring at the possibility of creating and operating hundreds of data connection pipes and processing the requisite legal agreements to do so.

The Advisory Group had significant discussions around the concept that this entity should be a contracted, neutral 3rd-party trusted data provider. The Advisory Group expects that discussions surrounding exactly what criteria should be in place for deciding who qualifies as a neutral 3rd-party provider will continue. Precedent exists in the area with the registrar data escrow program already in place to protect registrants in cases of registrar failure. A networking, security, data center or other managed services provider with high security data management practices, that routinely deals with providing restricted, contracted access to data sources, and no conflict of interest, is likely eligible. Extra care should be taken to avoid conflict of interest between the ZFAPP activities and affiliations of the party that provides such services.

For those models where a single entity is selected or created to consolidate all aspects of zone file data access by third parties, that entity is referred to as the **Zone File Access Program Provider** (ZFAPP). This entity would enter into agreements with all parties – registry operators and data consumers – and acts as the single contracting authority for both sides. The ZFAPP would also act as the data collection and/or distribution point, and provides end–user support to data subscribers.

In short, the ZFAPP acts as the intermediary between the domain registries and zone file consumers for all things related to zone file access. Multiple data access models are possible under the ZFAPP.

THE REPOSITORY MODEL -- In this model the ZFAPP would collect zone data files regularly from the registry operators, verify them, and publish them (possibly via a variety of transport technologies) via a single, secure platform for data subscribers. In this model, high performance, high security, data validation, and potentially additional services could be offered with consolidation of actual data files at the ZFAPP.

For example, the ZFAPP could offer “data normalization” (e.g. deliver all zones using a specific compression technique or file format) or it might provide resource record filtering capabilities for data consumers who might have no use for (e.g. DNSSEC resource records) and would benefit from the ability to indicate that such records be filtered from the zone data they gather from the ZFAPP.

THE PROXY MODEL -- In this model, the ZFAPP operates something like an SSL VPN application proxy used by organizations to protect intranets and extranets. The ZFAPP provides a single secure access point for zone file consumers., The ZFAPP authenticates zone file consumers, accepts requests for

zone data from a registry, verifies the consumer is authorized to access the indicated registry's zone, and then proxies the request and subsequent data connections back to the designated registry. This model is distinguished from the repository model with respect to "zone data at rest." In particular, the registry derives many of the same benefits (other than lower bandwidth and new services) but does not have to share its data with another "centralized" party.

In this approach, the ZFAPP does not store zone files locally but requests these from the registry operator as consumer requests arrive. Concurrency issues between registry operator and ZFAPP "copies" of zone data may be reduced or eliminated at the expense of more frequent downloads from registry to ZFAPP (note that some form of caching at the ZFAPP might also be appropriate). Normalization might still be performed "on the fly" and filtering could still be offered.

THE CLEARINGHOUSE MODEL -- A third approach is to create a centralized point -- ZFAPP -- through which a consumer of Zone File data can apply for access to registry zone files. In this case, the ZFAPP maintains the account credentials (identities, passwords, IPs, etc.) and distributes it to all the registries, but registries still provide their own FTP servers to download the data. In this model, registries are relieved of most of the burden of manual account setup.

7.1.3 Registry operations/relationships with the ZFAPP -- Repository and Proxy Models

Registry relationship and operations with the ZFAPP:

1. An entity is chosen to be the ZFAPP through a RFP-contracting process.
2. The ZFAPP enters into contracts with all gTLD registries to manage the zone-- file access program on their behalf to data consumers.
3. Each data consumer signs a contract with the ZFAPP, designating which zone files they wish to access.
4. The ZFAPP maintains and updates all contracts as necessary to reflect changing requirements and contracted parties.
5. The ZFAPP creates a highly secure data services operation to host the zone files for the registries and establishes secure channels for gTLD operators so that it can upload zone files to the central repository on a daily basis[repository model]. --OR-- The ZFAPP creates a highly secure data proxy system to allow secure back-end pass--through connections to the registries for data file transfer through to the data consumer [proxy model].
6. The gTLD registries and the ZFAPP monitor the integrity of the transmitted zone file to ensure it is accurate before releasing to the subscriber base.
7. Problems reported by data consumers that point to issues with particular zone file data are confirmed by the ZFAPP and transmitted back to the relevant gTLD operator for resolution.

7.1.4 Consumer operations /relationships with a ZFAPP -- Repository and Proxy Models

Data client relationship and operations with the ZFAPP:

1. A universal contract is created for use by data subscribers, including selection of the gTLDs the data client wishes to access.

2. ZFAPP, gTLD registries and consumers enter into contractual relationships. Such can be construed of bilateral or trilateral agreements that provide mechanisms for registries to monitor access to zone file and enforce the terms of the zone file access program.
3. The ZFAPP provides access credentials to data subscribers.
4. A methodology to maintain access credentials is provided by the ZFAPP.
5. The ZFAPP maintains a secure, transaction limited access methodology for the data subscribers to obtain their contracted zone files.
6. The ZFAPP provides methodologies to ensure the integrity of the data transmission and allow for updates/corrections if there is a problem.
7. The ZFAPP maintains a service center to assist data clients with problem resolution.
8. The ZFAPP watches for abusive behavior and is authorized to suspend access for clients found to be abusing the system

7.2 ZFA Model Comparison

Issue	Current ZFA Practice	Enhanced Bi-Lateral	ZFAPP Clearinghouse	ZFAPP Repository	ZFAPP Proxy
ZFA Agreement	Separate agreement for each registry			Universal agreement (possible to add registry specific clauses for unique requirements)	
- Creation and maintenance					
- distribution, review countersign					
- secure archival of agreements					
- change management					
Zone File Distribution	Registry transfers zone files to "n" consumers			Registry transfers zone files to ZFAPP	Registry transfers zone files to ZFAPP and ZFAPP transfers zones in real time to consumer
Zone File Hosting	Registry hosts zone files			ZFAPP maintains local copies of zone files	ZFAPP proxies connection requests to registry; only registry hosts zone files
FTP Server Operations					
- redundancy & availability	Each registry handles operations directly	Each registry handles operations directly; common standard for protocol and file naming	Each registry handles operations directly	FTP service must satisfy SLAs established for ZFAPP. All consumer contracted zones downloaded via a single service point (one address/netblock); registries have "one" customer.	
- performance metrics (e.g. SLAs)					
- bandwidth, connection speeds					
- new data transfer strategies	Each registry could adopt new methods independently			ZFAPP can assess/introduce high performance data transfer alternatives without change to existing registry operations	ZFAPP can assess/introduce high performance data transfer alternatives without change to existing registry operations (however, "registry facing improvements require changes to registry operations)

Issue	Current ZFA Practice	Enhanced Bi-lateral	ZFAPP Clearinghouse	ZFAPP Repository	ZFAPP Proxy
<p>Server and Access Security</p> <ul style="list-style-type: none"> - hardening of public facing systems - monitoring and problem resolution - credential creation, recovery and reset - auditing of customer access - abuse monitoring and reporting - access and origin controls - firewall, IDS, DoS defense, etc. 	<p>Each registry handles these processes directly</p>		<p>Hybrid Approach – ZFAPP handles some security processes; registry handles other processes directly</p>	<p>Uniform security, ZFAPP contracted to meet security best practices, registries only need to permit access from ZFAPP. ZFAPP enforces uniform abuse policy across all zone file accesses.</p>	
<p>Helpdesk and Customer Care</p>	<p>Varies across registries</p>		<p>Hybrid Approach – ZFAPP handles some helpdesk processes; registry handles other processes directly</p>	<p>Must satisfy ZFAPP SLA for accessibility, availability, responsiveness. Single PoC for consumers to resolve difficulties, service outage. ZFAPP resolves back-end</p>	

7.3 Four ZFA Models: Advantages and Disadvantages

Issue	Current ZFA Practice	Enhanced Bi-lateral	ZFAPP Clearinghouse	ZFAPP Repository	ZFAPP Proxy
Advantages	<ul style="list-style-type: none"> § Current systems in place 	<ul style="list-style-type: none"> § Consistent access methodology § Potential improvements in transport and delivery 	<ul style="list-style-type: none"> § Scale handled by a single point of contact § Potential improvements in transport and delivery § Single account administration § Registry retains control of transport/delivery § Administrative/Legal "One stop shop" for consumers of ZFA data § Registry retains right to enforce/terminate zone file agreements § Lower costs to consumer and provider of zone file data § Normalization or filtering of the data could be provided 	<ul style="list-style-type: none"> § Scale handled by a single point of contact § Potential improvements in transport and delivery § "One stop shop" for consumers of ZFA data § Ability to track/audit users over multiple zones (anti-abuse) § Lower costs to consumers and providers of ZFA data § Registry retains right to enforce/terminate zone file agreements § Lower costs to consumer and provider of zone file data § Normalization or filtering of the data could be provided § Reduces bandwidth requirements for registry operators 	<ul style="list-style-type: none"> § Scale handled by a single point of contact § Potential improvements in transport and delivery § Registry retains control of transport/delivery § Administrative/Legal "One stop shop" for consumers of ZFA data § Registry retains right to enforce/terminate zone file agreements § Lower costs to consumer and provider of zone file data § Normalization or filtering of the data could be provided
Disadvantages	<ul style="list-style-type: none"> § Does not scale with the introduction of large number of TLDs § Widely varying access methodologies § Inconsistent security approaches § Multiple legal/admin points of contact § Higher costs for both providers and consumers 	<ul style="list-style-type: none"> § Scaling problem not solved for introduction of large number of TLDs § Cost model does not change from current ZFA practice 	<ul style="list-style-type: none"> § Need for re-examination and amendment of Zone File Access Agreement? 	<ul style="list-style-type: none"> § Need for re-examination and amendment of Zone File Access Agreement? § ZFA Data latency 	<ul style="list-style-type: none"> § Need for re-examination and amendment of Zone File Access Agreement?

7.4 Cost Models for Alternative Zone File Access Strategies

During its early work on ZFA, the Advisory Group recognized that modeling the cost of both provisioning and accessing the data would be essential. A small subgroup of the Advisory Group was convened to develop an initial model. Outreach was conducted to existing gTLD registries to understand provider costs and numerous data consumers in the group contributed to the development of the consumer cost model. The goals of the model were to better understand the economic implications of extending the current scheme of ZFA to larger numbers of gTLDs – and to compare that strategy to ZFAPP entity alternatives. Such a model is intended to understand these implications from both the perspective of providers and consumers of zone file data.

The model (available at the ZFA Advisory Group’s web page at: <http://www.icann.org/en/topics/new-gtlds/zone-file-access-en.htm>) examines costs for all participants in both today’s environment and in a projected scenario with the presences of a greatly expanded root zone. The principal conclusion from this analysis is that there are increased costs for both consumers and providers of ZFA in a root zone with a much larger number of gTLDs. In fact, compared to the current costs, and assuming costs are imposed on the consumer, consumers of zone file data would see a substantial increase in costs when they are faced with a significantly larger number of gTLDs. Another feature of the model is that it focuses on incremental costs only – it does not address startup costs related to bringing one a ZFA entity into operation.

It is important to note that the model is built on a set of assumptions. Part of the purpose of having a model in the first place is to test it under different sets of assumptions about the subscription model, the presence of DNSSEC and how the model is transported. The model can be downloaded and modified based on different reasoning for each of the underlying assumptions. The subgroup that created the model recognizes it as a first attempt to provide an economic analysis of the zone file access infrastructure. As a result, the early assumptions were conservative in nature. Some in the subgroup believe that the real costs, especially for consumers of zone file data, are much larger than specified here. Because of this, the subgroup is looking forward to further discussions in the Advisory Group about the model and its underlying parameters. Based on both Advisory Group and public comment, they expect to significantly refine the model.

In any event, the model shows that there is clear evidence that simply extending the current bi-lateral model for zone file access raises a serious set of economic concerns; especially for ZFA consumers.

7.5 Funding Models for gTLD Zone File Access

Funding for a ZFA provider/entity requires dealing with two sets of requirements: funding at startup and the cost of ongoing operations. Even though a particular model for ZFA provision is not selected, it is still possible to examine some of the options related to funding requirements.

7.5.1 Funding Scenarios for ZFA Consumers

There are three principal models for setting goals for consumer costs related to ZFA:

- **No cost** – this model maintains the existing regime of “free” access to all consumers of the ZFA data. It is recognized that the access is not actually free (there are administrative, maintenance, and infrastructure costs as an example), but no money passes between the provider and consumer of the data. This is consistent with the existing registry agreement and continues a long-held practice of providing zone file data to any consumer who requests it.
- **Low/No fee** – the idea would be to provide tiered access to the data. Some consumers would be given access on a no cost model, but others would be charged as a way to develop revenue for the provision of the ZFAPP. What categories would be in place and how consumers would be assigned to those categories is an open question.
- **Market rate** – this model would support a “market” based approach to pricing access to the zone file data.

In the event that consumers were asked to pay for zone file access there are several business models for the payments:

- Consumers could be asked to pay a one-time fee (especially in the instance where the economic model showed that the largest cost is associated with initial provisioning of an account);
- Consumers could pay a fixed, annual fee as a mechanism for providing funding for ongoing operations; or,
- Consumers could pay a transactional fee associated with the individual downloads of the zone file data.

Clearly, other models and combinations are possible depending on the goal that was established for the funding.

7.5.2 Funding Scenarios for ZFA Providers

Two alternative goals for providers of ZFA data are possible: either a new strategy for ZFA provisioning should result in no increase in costs to providers or the new strategy should result in lower costs to providers. Each of the models has varying potential for changing the cost model for providers. In an optimal model, the costs to the provider may be lowered through consistency of access or centralized administration.

7.5.3 ZFAPP Operational Model

There are a wide variety of organizational models that could be used to set up a ZFAPP entity. Decisions about the operational model include whether or not the ZFAPP would be a for-profit or non-profit entity, whether or not the ZFAPP could be part of a larger organization and whether or not the organization was strictly built around a cost-recovery model. In any case, careful thought must be given to the restrictions that are imposed on the operations of the ZFAPP. For instance, the ZFAPP might have to be contractually limited in what they can and cannot provide as a way to ensure that they do not compete with value-added services that are offered by other providers

There are also several possibilities for funding a ZFAPP. As an example, registry fees (that are lower as a result of the ZFAPP operation) could be used to fund the operations of the ZFAPP. Or, the consumers of the ZFAPP could fund the ongoing operations of the ZFAPP. Any funding model has to match the goals

for ZFA consumers and providers – some choices of funding goals will limit ZFAPP funding alternatives. In the model where revenue would be generated, it might be possible to compensate registries for work done to make zone files available. However, there are many open question about how that might be done (e.g. match compensation size to the size of the zone provided, set limits on compensation provided, or size compensation by how often the zone file was accessed).

7.6 Issues Addressed in a Third Party ZFA System

The goal of a ZFAPP system is to alleviate a number of issues for both gTLD registries and data consumers. The perceived benefits from the creation of such a provider are (a) reduced costs associated with systems and bandwidth capacities and (b) reduced demands on the time of support or systems personnel. The ZFAPP also has the potential to increase data accuracy, data usability and availability, enhance security, and lower liability exposures. These benefits are derived from a simplified, better-controlled dissemination of zone file data.

7.6.1 gTLD Operator Benefits

The benefits of a third party ZFA system to a gTLD operator might include the following:

- 1) Single legal agreement with ZFAPP.
 - a) Registries do not need to spend time or money on maintaining, updating, or archiving zone data consumer contracts for zone file access.
 - b) Registries do not need to worry about communicating changes and tracking acceptance if updates to the zone data consumer contract are needed.
- 2) Single, secure connection with the ZFAPP
 - a) Potential to reduce investments in multiple, high--capacity lines or servers for simultaneous downloads to hundreds of subscribers [repository model].
 - b) Uniformly secured and auditable transmission of data.
 - c) A single contracted party assures that the integrity of distributed zone files on behalf of all registries [repository model].
 - d) Registries only have to deal with a single point of contact (ZFAPP) for zone file access related problems.
 - e) Trusted third party is responsible for change control, i.e., changes to data clients' changing network architecture that require updates to access control lists (ACL's).
 - f) Trusted third party manages data consumer credential creation or management for end-users.
 - g) Trusted third party buffers registry systems from attack. Registry operator is no longer exposed to attacks against zone file download systems.
- 3) ZFAPP handles zone file consumer support questions and problem resolution
- 4) ZFAPP polices data access and handles abuse issues
 - a) Registries benefit from 3rd party monitoring for abuse and gaming of service.
 - b) Registry customer support and legal staff time is reduced.

7.6.2 Zone File Consumer Benefits

The benefits of a third party ZFA system to a zone file consumer may include the following:

- 1) Single legal agreement with ZFAPP.
 - a) One process to go through for obtaining access instead of potentially hundreds.
 - b) Zone file consumers do not need to spend time or money on maintaining, updating or archiving registry contracts for zone file access.
- 2) Single, secure connection with the ZFAPP
 - a) Zone file consumers do not need to support multiple servers, access methods, connection automation for downloads from hundreds of registries.
 - b) Zone file consumers deal with a single access control policy.
 - c) ZFAPP provides a single access method and framework for secure and auditable transmission of zone data.
 - d) ZFAPP assures that the distributed zone files are downloaded without error.
 - e) Problems resolution is directed to a single (ZFAPP) point of contact.
 - f) Changes to the zone file consumer's network architecture that affect zone file access are process for all registries through a single (ZFAPP) point of contact.
 - g) The ZFAPP can implement new forms of data transfer easily – e.g. web services – across all registries using a single platform for all services.
 - h) Zone file access account (identity) management is centralized and managed by ZFAPP.
 - i) Single (common) provider is better able to accommodate easy migration to higher security models (e.g. multi- -factor authentication) in the future.
- 3) ZFAPP acts as the registry operators' outsourced agent on operational issues
 - a) ZFAPP assures the availability of the latest zone file via its direct relationship with the registries.
 - i) ZFAPP manages access, accuracy and concurrency and is thus positioned to detect and correct problems before the data client even knows they occurred.
 - ii) Zone data consumer does not have to chase down problems with individual registries.
 - b) ZFAPP handles support questions and access problems for all registry files
 - i) Single point of contact available 24/7 (or higher than most today)
 - c) Service level agreements with ZFAPP can assure that issues are dealt with quickly (defined by metric) since an error in one file will affect many, allowing the ZFAPP to act with registry with authority.

8.0 NO EFFECT ON ENHANCED REGISTRY SERVICES

No change is required for registry—specific services like access to “rapid” zone updates, “who – was” services, or other enhanced data services gTLD registries currently offer or contemplate. This proposal is targeted solely at the required daily zone file download. Other services offered by registries would continue to be handled directly by them. Such services may well benefit from resources being freed up from supporting the daily zone access.

9.0 POTENTIAL FOR ENHANCED DATA SERVICES

Providing better access may increase the number of data subscribers for daily updates. Exposure to that data may well make it easier for innovative registry operators to provide enhanced services to

direct or even indirect customers. For registry operators with direct service offerings, a wider use of accurate zone file data may provide a larger potential sales base of consumers and may help to identify customers who would subscribe to registry services that provide information beyond the daily zone transfers. The consolidation of data from all gTLD zones into a single location may provide the opportunity, if allowed, for registries to share in profiting from enhanced services offered through that outlet.

ANNEX A – PARTICIPANTS IN THE ZONE FILE ACCESS ADVISORY GROUP

Mike O'Connor	O'Connor Company of St Paul
John Levine	Taughannock Networks
Nacho Amadoz	Fundacio puntCAT (.CAT)
Adam Palmer	Symantec
David Maher	Public Interest Registry (.ORG)
Vladimir Shadrinov	Telnic (.TEL)
Brian Cute	Afilias (.INFO)
Tom Barrett	EnCirca - ICANN-accredited Registrar
Paul Stahura	
Rick Wilhelm	Network Solutions - ICANN-accredited Registrar
Tatyana Khramtsova	RU-Center, Registrar
Rod Rasmussen	President/CEO, Internet Identity
Rod Dixon	Attorney
Joe St Sauver	Internet2 and the University of Oregon
Wang Wei	CNNIC - ccTLD Registry
John Kristoff	Research Analyst, Team Cymru
Jothan Frakes	Minds + Machines
Ken Stubbs	Afilias (.INFO)
Asif Kabani	International Sustainable Development – Resource Centre (ISD-RC)
Berry Cobb	Owner, Infinity Portals, LLC
Susan Prosser	DomainTools
John McCormac	Hosterstats.com

ICANN

Francisco Arias
Mark McFadden
Dave Piscitello
Kurt Pritz
Craig Schwartz

ANNEX B – TYPICAL ZONE FILE ACCESS AGREEMENT

1. PARTIES

The User named in this Agreement hereby contracts with the gTLD Registry for a non-exclusive, non-transferable, limited right to access an Internet host server or servers designated by the gTLD Registry from time to time, and to transfer a copy of the described Data to the User's Internet host machine specified below, under the terms of this Agreement. Upon execution of this Agreement by the gTLD Registry, the gTLD Registry will return a copy of this Agreement to you for your records with your UserID and Password entered in the spaces set forth below.

2. USER INFORMATION

(a) User: _____

(b) Contact Person: _____

(c) Street Address: _____

(d) City, State or Province: _____

(e) Country and Postal Code: _____

(f) Telephone Number: _____

(including area/country code)

(g) Fax Number: _____

(including area/country code)

(h) E-Mail Address: _____

(i) Specific Internet host machine which will be used to access the gTLD Registry's server to transfer copies of the Data:

Name: _____

IP Address: _____

(j) Purpose(s) for which the Data will be used: During the term of this Agreement, you may use the data for any legal purpose, not prohibited under Section 4 below. You may incorporate some or all of the Data in your own products or services, and distribute those products or services for a purpose not prohibited under Section 4 below.

3. TERM

This Agreement is effective for a period of three (3) months from the date of execution by the gTLD Registry (the "Initial Term"). Upon conclusion of the Initial Term, this Agreement will automatically renew for successive three-month renewal terms (each a "Renewal Term") until terminated by either party as set forth in Section 12 of this Agreement or one party provides the other party with a written notice of termination at least seven (7) days prior to the end of the Initial Term or the then current Renewal Term.

NOTICE TO USER: CAREFULLY READ THE FOLLOWING TERMS AND CONDITIONS. YOU MAY USE THE USER ID AND ASSOCIATED PASSWORD PROVIDED IN CONJUNCTION WITH THIS AGREEMENT ONLY TO OBTAIN A COPY OF TOP-LEVEL DOMAIN ("TLD")

ZONE FILES, AND ANY ASSOCIATED ENCRYPTED CHECKSUM FILES (COLLECTIVELY THE "DATA"), VIA THE FILE TRANSFER PROTOCOL ("FTP") OR HYPERTEXT TRANSFER PROTOCOL ("HTTP") PURSUANT TO THESE TERMS.

4. GRANT OF ACCESS

the gTLD Registry grants to you a non-exclusive, non-transferable, limited right to access an Internet host server or servers designated by the gTLD Registry from time to time, and to transfer a copy of the Data to the Internet host machine identified in Section 2 of this Agreement no more than once per 24 hour period without the express prior written consent of the gTLD Registry using FTP or HTTP for the purposes described in this Section 4. You agree that you will:

(a) use this Data only for lawful purposes but that under no circumstances will you use this Data to: (1) allow, enable, or otherwise support any marketing activities, regardless of the medium used. Such media include but are not limited to e-mail, telephone, facsimile, postal mail, SMS, and wireless alerts; or (2) enable high volume, automated, electronic processes that send queries or data to the systems of the gTLD Registry or any ICANN-accredited registrar, except as reasonably necessary to register domain names or modify existing registrations. The gTLD Registry reserves the right, with the approval of the Internet Corporation for Assigned Names and Numbers ("ICANN"), to specify additional specific categories of prohibited uses by giving you reasonable written notice at any time and upon receiving such notice you shall not make such prohibited use of the Data you obtain under this Agreement.

(b) copy the Data you obtain under this Agreement into a machine-readable or printed form only as necessary to use it in accordance with this Agreement in support of your use of the Data.

(c) comply with all applicable laws and regulations governing the use of the Data.

(d) not distribute the Data you obtained under this Agreement or any copy thereof to any other party without the express prior written consent of the gTLD Registry, except that you may redistribute the Data insofar as it has been incorporated by you into a value-added product or service that does not permit the extraction of a substantial portion of the Data from the value-added product or service, provided you prohibit the recipient of the Data from using the Data in a manner contrary to Section 4(a).

(e) take all reasonable steps to protect against unauthorized access to, use, and disclosure of the Data you obtain under this Agreement.

5. FEE

You agree to remit in advance to the gTLD Registry a quarterly fee of \$0 (USD) for the right to access the files during either the Initial Term or Renewal Term of this Agreement. The gTLD Registry reserves the right to adjust, with the approval of ICANN, this fee on thirty days' prior notice to reflect a change in the cost of providing access to the files.

6. PROPRIETARY RIGHTS

You agree that no ownership rights in the Data are transferred to you under this Agreement. You agree that any copies of the Data that you make will contain the same notice that appears on and in the Data obtained under this Agreement.

7. METHOD OF ACCESS

The gTLD Registry reserves the right, with the approval of ICANN, to change the method of access to the Data at any time. You also agree that, in the event of significant degradation of system processing or other emergency, the gTLD Registry may, in its sole discretion, temporarily suspend access under this Agreement in order to minimize threats to the operational stability and security of the Internet.

8. NO WARRANTIES

The Data is being provided "as-is." The gTLD Registry disclaims all warranties with respect to the Data, either expressed or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, and non-

infringement of third party rights. Some jurisdictions do not allow the exclusion of implied warranties or the exclusion or limitation of incidental or consequential damages, so the above limitations or exclusions may not apply to you.

9. SEVERABILITY

In the event of invalidity of any provision of this Agreement, the parties agree that such invalidity shall not affect the validity of the remaining provisions of this Agreement.

10. NO CONSEQUENTIAL DAMAGES

In no event shall the gTLD Registry be liable to you for any consequential, special, incidental or indirect damages of any kind arising out of the use of the Data or the termination of this Agreement, even if the gTLD Registry has been advised of the possibility of such damages.

11. GOVERNING LAW

This Agreement shall be governed and construed in accordance with the laws of the [insert locale]. You agree that any legal action or other legal proceeding relating to this Agreement or the enforcement of any provision of this Agreement shall be brought or otherwise commenced only in the state or federal courts in [insert locale] and the [insert locale]. You expressly and irrevocably agree and consent to the personal jurisdiction and venue of the federal and states courts located [insert locale] (and each appellate court located therein) for matters arising in connection with this Agreement or your obtaining, use, or distribution of the Data.

12. TERMINATION

You may terminate this Agreement at any time by erasing the Data you obtained under this Agreement from your Internet host machine together with all copies of the Data and providing written notice of your termination to the gTLD Registry at [insert gTLD Registry Address]. The gTLD Registry has the right to terminate this Agreement immediately if you fail to comply with any term or condition of this Agreement. You agree upon receiving notice of such termination of this Agreement by the gTLD Registry or expiration of this Agreement to erase the Data you obtained under this Agreement together with all copies of the Data.

13. DEFINITION

"Data" means all data contained in a DNS zone file for the Registry TLD as provided to TLD nameservers on the Internet.

14. ENTIRE AGREEMENT

This is the entire agreement between you and the gTLD Registry concerning access and use of the Data, and it supersedes any prior agreements or understandings, whether written or oral, relating to access and use of the Data.