4. Performance Specifications

4.1 Goals and intentions of Service Level Agreements and Public Service Monitoring

Goals of Service Level Agreements:

Service Level Agreements are set between ICANN and Registry Operators to ensure predictable consistent delivery and availability of Registry Services. Services fall into to two basic categories, publicly available services and services between contracted parties. Traditional Whois services also known as Registration Data Publication Services or RDPS and DNS (Domain Name Service) are public services. EPP Services, which are provisioned between Registrars and Registries, are services between contracted parties.

Goals of Public Service Monitoring:

The primary purpose of monitoring is to identify potential issues with the availability of public services, in conformance with ensuring the security and stability of the DNS. Monitoring works in conjunction with well understood issue escalation, issue confirmation, and issue remediation procedures established with Registry Operators.

Public Services:

Availability of DNS is essential to the operational stability of the Internet. Availability of RDPS services is considered essential by many stakeholders in law enforcement and legal communities. Monitoring availability of these services is a difficult challenge as they are both offered in Anycast environments, which can incorporate numerous valid service addresses where each service address can in turn represent a "mesh" of many geographically distributed physical service nodes. These Anycast meshes can dynamically change their arrangements of geographically distributed service nodes for numerous operational purposes. Registry Operators are tasked with providing DNS and RDPS services over public networks over which they have no control.

DNS is absolutely required for the Internet to operate as intended. Monitoring must be conducted inclusively of public network overhead in order to confirm basic public availability. Contractual obligations associated with DNS SLAs must take into account the effect of public networks that are beyond the control of the Registry Operator.

Many stakeholders consider RDPS an essential service. However availability of RDPS is not required for basic operation of the Internet as designed. Monitoring must be conducted inclusively of public network overhead in order to confirm basic public availability. Contractual obligations associated with RDPS SLAs must take into account the effect of public networks that are beyond the control of the Registry Operator.

Services between Contracted Parties:

EPP (Extensible Provisioning Protocol) Registry transactions support the creation, deletion and change management of domain names strictly between Registrars and Registries. Availability of these services to Registrants depends on the availability of Contracted Party Services. If the Registrant cannot access Registrar services, the Registrant cannot create, delete or manage changes to domains. Contractual obligations associated with EPP Registry transaction SLAs should be addressed between Registrars and Registries. Registrars and Registries should have appropriate escalations available with ICANN should

resolution over SLA issues between these parties be identified as unresolvable by either party (See Section 6 escalations).

4.2 Definitions

Contracted Party Services. This term refers generically to the services offered under direct party to party contract, maintained between Registry Operators and Registrars that directly relate to registration management in ICANN Top Level Domain Registries.

Formatted: Font: Not Bold

DNS. Refers to the Domain Name System as specified in RFCs 1034, 1035 and related RFCs.

DNS name server availability. Refers to the ability of a public-DNS registered "**IP address**" of a particular name server (also known as a "service address") listed as authoritative for a domain name~~,~~ to answer DNS queries from an Internet user~~. All the public-DNS registered "**IP address**" of all name servers of the domain name being monitored shall be tested individually. If 51% or more of the DNS testing probes get undefined results from "**DNS tests**" to a name server "**IP address**" over any of the transports (UDP or TCP) during a given time, the name server "**IP address**" will be considered unavailable~~.

DNS probes. Probes used for applying DNS tests (see above) that are located at numerous global locations.

DNS resolution RTT. Refers to either "**UDP DNS resolution RTT**" or "**TCP DNS resolution RTT**".

DNS service availability. Refers to the ability of the group of listed-as-authoritative name servers of a particular domain name (e.g~~. a TLD), to answer DNS queries from an Internet user. For the service to be considered available at some point in time, at least, two of the name servers registered in the DNS must have defined results from "**DNS tests**" to each of their public-DNS registered "**IP addresses**" over both (UDP and TCP) transports. If 51% or more of the DNS testing probes see the service as unavailable over any of the transports (UDP or TCP) during a given time, the DNS service will be considered unavailable.~~., a TLD), to answer DNS queries from an Internet user.

DNS test. Means one non-recursive DNS query sent to a particular "**IP address**" (via UDP or TCP). If DNSSEC is offered in the queried DNS zone, for a query to be considered answered, the signatures must be positively verified against a corresponding DS record published in the parent zone or, if the parent is not signed, against a statically configured Trust Anchor. See Appendix 1 for specifics of the required method. ~~The query shall be about existing domain names. The answer to the query must contain the corresponding information from the Registry System, otherwise the query will be considered unanswered. If the answer to a query has the TC bit set, the query will be considered unanswered. A query with a "**DNS resolution RTT**" 5 times higher than the corresponding SLR, will be considered unanswered. The possible results to a DNS test are: a number in milliseconds corresponding to the "**DNS resolution RTT**" or, undefined/unanswered.~~

DNS update time. Refers to the time measured from the reception of an EPP confirmation to a transform command on a domain name~~, up until all the name servers of the parent domain name answer "**DNS queries**" with data consistent with the change made. This only applies for changes to DNS information~~ to the initiation of related changes to relevant DNS data offered from the Registry's DNS service addresses.

EPP. Refers to the Extensible Provisioning Protocol as specified in RFC 5730 and related RFCs.

EPP command RTT. Refers to "**EPP session-command RTT**", "**EPP query-command RTT**" or "**EPP transform-command RTT**".

EPP query-command RTT. Refers to the **RTT** of the sequence of packets that includes the sending of a query command plus the reception of the EPP response for only one EPP query command. It does not include packets needed for the start ~~nor~~ or close of ~~neither~~either the EPP ~~nor~~or the TCP session. EPP query commands are those described in section 2.9.2 of EPP RFC 5730. ~~If the **RTT** is 5 times or more the corresponding SLR, the **RTT** will be considered undefined.~~

EPP service availability. Refers to the ability of the TLD EPP servers as a group, to respond to commands from the Registry accredited Registrars, who already have credentials to the servers. ~~The response shall include appropriate data from the Registry System. An EPP command with "**EPP command RTT**" 5 times higher than the corresponding SLR will be considered as unanswered. For the EPP service to be considered available at during a measurement period, at least, one IPv4 and one IPv6 (if EPP is offered over IPv6) address of the set of EPP servers must have defined results from "**EPP tests**". If 51% or more of the EPP testing probes see the EPP service as unavailable during a given time, the EPP service will be considered unavailable.~~

EPP session-command RTT. Refers to the **RTT** of the sequence of packets that includes the sending of a session command plus the reception of the EPP response for only one EPP session command. For the login command it will include packets needed for starting the TCP session. For the logout command it will include packets needed for closing the TCP session. EPP session commands are those described in section 2.9.1 of EPP RFC 5730. ~~If the **RTT** is 5 times or more the corresponding SLR, the **RTT** will be considered undefined.~~

EPP test. Means one EPP command sent to a particular "**IP address**" for one of the EPP servers. Query and transform commands, with the exception of "create", shall be about existing objects in the Registry System. The response shall include appropriate data from the Registry System. The possible results to an EPP test are: a number in milliseconds corresponding to the "**EPP command RTT**" or undefined/unanswered.

EPP transform-command RTT. Refers to the **RTT** of the sequence of packets that includes the sending of a transform command plus the reception of the EPP response for only one EPP transform command. It does not include packets needed for the start ~~nor~~ or close of ~~neither~~either the EPP ~~nor~~or the TCP session. EPP transform commands are those described in section 2.9.3 of EPP RFC 5730. ~~If the **RTT** is 5 times or more the corresponding SLR, the **RTT** will be considered undefined.~~

IP address. Refers to IPv4 or IPv6 address without making any distinction between the two. When there is need to make a distinction, IPv4 or IPv6 is mentioned.

Public Services. This term refers to critical services in the active resolution of domain registrations in ICANN Top Level Domain Registries, that are directly consumed by the general public.

RDPS. Registration Data Publication Services refers to the collective of WHOIS and Web based WHOIS services as defined in "SPECIFICATION 4" of this Agreement.

RDPS availability. Refers to the ability of all the RDPS services for the TLD~~,~~ to respond to queries from an Internet user with appropriate data from the relevant Registry System. ~~For the RDPS to be considered available at some point in time, one IPv4 and one IPv6 address for each of the RDPS services must have defined results from "**RDPS tests**". If 51% or more of the RDPS testing probes see any of the RDPS services as unavailable during a given time, the RDPS will be considered unavailable.~~

RDPS query RTT. Refers to the collective of "**WHOIS query RTT**" and "**Web-based-WHOIS query RTT**".

RDPS test. Means one query sent to a particular "**IP address**" for one of the servers of one of the RDPS services. ~~Queries shall be about existing objects in the Registry System and the responses must contain the corresponding information otherwise the query will be considered unanswered. Queries with an **RTT** 5 times higher than the corresponding SLR will be considered as unanswered. The possible results to an RDPS test are: a number in milliseconds corresponding to the **RTT** or undefined/unanswered.~~

RDPS update time. Refers to the time measured from the reception of an EPP confirmation to a transform command on a domain name~~, up until all~~ to the ~~"**IP addresses**"~~initiation of ~~all~~relevant data updates offered by the ~~servers of all the~~Registry's RDPS services ~~reflect the changes made.~~.

RTT. Round-Trip Time or **RTT** refers to the time measured from the sending of the first bit of the first packet of the sequence of packets needed to make a request until the reception of the last bit of the last packet of the sequence needed to receive the response. If the client does not receive the whole sequence of packets needed to consider the response as received, the time will be considered undefined.

SLR. Service Level Requirement is the level of service expected for a certain parameter being measured in a ~~Server~~Service Level Agreement (SLA).

TCP DNS resolution RTT. Refers to the **RTT** of the sequence of packets from the start of the TCP connection to its end, including the reception of the DNS response for only one DNS query. ~~If the **RTT** is 5 times or more the corresponding SLR, the **RTT** will be considered undefined.~~

UDP DNS resolution RTT. Refers to the **RTT** of the sequence of two packets, the UDP DNS query and the corresponding UDP DNS response. ~~If the **RTT** is 5 times or more the corresponding SLR, the **RTT** will be considered undefined.~~

Web-based-WHOIS query RTT. Refers to the **RTT** of the sequence of packets from the start of the TCP connection to its end, including the reception of the HTTP response for only one HTTP request. ~~If Registry Operator implements a multiple-step process to get to the information, only the last step shall be measured. If the **RTT** is 5 times or more the corresponding SLR, the **RTT** will be considered undefined.~~

WHOIS query RTT. Refers to the **RTT** of the sequence of packets from the start of the TCP connection to its end, including the reception of the WHOIS response. ~~If the **RTT** is 5 times or more the corresponding SLR, the **RTT** will be considered undefined.~~

4.3 Service Level Matrix

Availability and Response Metrics:

	Parameter	SLR (monthly basis)
DNS	DNS service availability	0 min downtime = 100% availability
	DNS name server availability	≤ 432 min of downtime (≈ 99%)
	TCP DNS resolution RTT	≤ 1500 ms, for at least 95% of the queries
	UDP DNS resolution RTT	≤ 400 ms, for at least 95% of the queries
	DNS update time	≤ 60 min, ~~for at least~~to initiate 95% of the updates

RDPS	RDPS availability	≤ 432 min of downtime (≈ 99%)
	RDPS query RTT	≤ 1500 ms, for at least 95% of the queries
	RDPS update time	≤ 60 min, ~~for at least~~to initiate 95% of the updates
EPP	EPP service availability	≤ 864 min of downtime (≈ 98%)
	EPP session-command RTT	≤ 3000 ms, for at least 90% of the commands
	EPP query-command RTT	≤ 1500 ms, for at least 90% of the commands
	EPP transform-command RTT	≤ 3000 ms, for at least 90% of the commands

Maintenance windows. Registry ~~Operators~~Operator is encouraged to do its maintenance windows for the different services at the times and dates of statistically lower traffic for each service. ~~However, note that there is no provision for~~ Downtime will no longer be differentiated between planned and unplanned outages in calculating availability. Maximum periods of planned maintenance are set but are separate from SLA availability considerations. The service is either available for the required uptime or ~~similar,~~ not regardless of the reason for any downtime~~, be it for maintenance or due~~. Emergency considerations due to system failures ~~will be noted simply as downtime and counted for SLA purposes.~~are addressed through escalation procedures described in sections 4.4 and 4.6.

Emergency Thresholds:

Critical Function	Emergency Thresholds	
DNS service (all servers)	4-hour continuous downtime	4-hour downtime / week
DNSSEC proper resolution	4-hour continuous downtime	4-hour downtime / week
SRS (EPP)	5-day continuous downtime	5-day downtime / month
WHOIS/Web-based WHOIS	7-day continuous downtime	7-day downtime / month
Data Escrow	Failure of more than three sequential, incremental, or mix of full and incremental deposits triggers emergency escalation process. Failure of more than three sequential full deposits results in Breach of the Registry Agreement caused by missing escrow deposits as described in Specification 2, Part B, Section 6.	

Note: Planned Maintenances that extend beyond maximum periods will trigger the emergency escalation process, except where the Registry Operator has provided explicit notice of extended maintenances to affected Registrars and ICANN emergency operations departments (see section 6).

4.4 Test Methods: Public Services and Services between Contracted Parties

Test Methods for Public Services:

DNS service availability. Refers to the ability of the group of listed-as-authoritative name servers of a particular domain name (e.g~~.~~., a TLD), to answer DNS queries from an Internet user. For the service to be considered available at some point in time, at least~~,~~ two of the name servers registered in the DNS must have defined results from "**DNS tests**" to each of their public-DNS registered "**IP addresses**" over both (UDP and TCP) transports. If 51% or more of the DNS testing probes see the service as unavailable over any of the transports (UDP or TCP) during a given time, ~~the DNS service will be considered unavailable.~~an Emergency Escalation process will be initiated with the Registry Operator. If 100% of the DNS testing probes see the service as unavailable over any of the transports (UDP or TCP) AND the Registry Operator is UNABLE or UNWILLING to demonstrate through relevant logging or third-party

monitoring that the DNS service is available on at least one DNS service address, then the DNS service will be considered unavailable.

DNS name server availability. Refers to the ability of a public-DNS registered "**IP address**" of a particular name server (also known as a "service address") listed as authoritative for a domain name~~,~~ to answer DNS queries from an Internet user. ~~All the public-DNS registered "**IP address**" of all name servers of the domain name being monitored shall be tested individually. If 51% or more of the DNS testing probes get undefined results from "**DNS tests**" to a name server "**IP**~~At least one service **address**~~" over~~ must be available at any ~~of the transports (UDP or TCP) during a~~ given time~~, the name server "**IP address**" will be considered unavailable.~~ to consider DNS service available (see DNS service availability).

UDP DNS resolution RTT. Refers to the **RTT** of the sequence of two packets, the UDP DNS query and the corresponding UDP DNS response. If the **RTT** is 5-times or more the corresponding SLR, the **RTT** will be considered undefined.

TCP DNS resolution RTT. Refers to the **RTT** of the sequence of packets from the start of the TCP connection to its end, including the reception of the DNS response for only one DNS query. If the **RTT** is 5-times or more the corresponding SLR, the **RTT** will be considered undefined.

DNS test. Means one non-recursive DNS query sent to a particular "**IP address**" (via UDP or TCP). If DNSSEC is offered in the queried DNS zone, for a query to be considered answered, the signatures must be positively verified against a corresponding DS record published in the parent zone or, if the parent is not signed, against a statically configured Trust Anchor. The query shall be about existing domain names. The answer to the query must contain the corresponding information from the Registry System, otherwise the query will be considered unanswered. If the answer to a query has the TC bit set, the query will be considered unanswered. A query with a "**DNS resolution RTT**" 5-times higher than the corresponding SLR, will be considered unanswered. The possible results to a DNS test are: a number in milliseconds corresponding to the "**DNS resolution RTT**" or~~,~~ undefined/unanswered. See Appendix 1 for DNS test specifics.

Measuring DNS parameters. Every minute, every DNS probe shall make an UDP and a TCP "**DNS test**" to each of the public-DNS registered "**IP addresses**" of the name servers of the domain ~~named~~name being monitored. If a "**DNS test**" gets unanswered, the tested IP will be considered as unavailable for the corresponding transport (UDP or TCP) from that probe until it is time to make a new test. The minimum number of active testing probes to consider a measurement valid is 20 at any given measurement period, otherwise the measurements will be discarded and will be considered inconclusive; during this situation no fault will be flagged against the SLRs.

Placement of DNS probes. Probes for measuring DNS parameters shall be placed as near as possible to the DNS resolvers on the networks with the most users across the different geographic regions; care shall be taken not to deploy probes behind high propagation-delay links, such as satellite links. Every probe will have connectivity through multiple transit providers and rotate all DNS tests through each provider in rotation. If a DNS test fails through one transit provider, the DNS Probe will repeat the test in turn through all of the multiple transit providers and only register a failure if all transit providers fail. Each transit provider will represent a clear separate upstream network path divergent of the other transit providers.

RDPS service availability. Refers to the ability of all the RDPS services for the TLD, to respond to queries from an Internet user with appropriate data from the relevant Registry System. For the RDPS to be considered available at some point in time, one IPv4 and one IPv6 address for each of the RDPS

services must have defined results from "**RDPS tests**". . If 51% or more of the RDPS testing probes see the service as unavailable during a given time, an Emergency Escalation process will be initiated with the Registry Operator. If 100% of the RDPS testing probes see any of the RDPS services as unavailable during a given time, the relevant RDPS service will be considered unavailable.

WHOIS query RTT. Refers to the **RTT** of the sequence of packets from the start of the TCP connection to its end, including the reception of the WHOIS response. If the **RTT** is 5-times or more the corresponding SLR, the **RTT** will be considered undefined.

Web-based-WHOIS query RTT. Refers to the **RTT** of the sequence of packets from the start of the TCP connection to its end, including the reception of the HTTP response for only one HTTP request. If Registry Operator implements a multiple-step process to get to the information, only the last step shall be measured. If the **RTT** is 5-times or more the corresponding SLR, the **RTT** will be considered undefined.

RDPS test. Means one query sent to a particular "**IP address**" for one of the servers of one of the RDPS services. Queries shall be about existing objects in the Registry System and the responses must contain the corresponding information otherwise the query will be considered unanswered. Queries with an **RTT** 5-times higher than the corresponding SLR will be considered as unanswered. The possible results to an RDPS test are: a number in milliseconds corresponding to the **RTT** or undefined/unanswered.

Measuring RDPS parameters. Every minute, every RDPS probe shall randomly select one IPv4 and one IPv6 addresses from all the public-DNS registered "**IP addresses**" of the servers for each RDPS service of the TLD being monitored and make an "**RDPS test**" to each one. If an "**RDPS test**" gets unanswered, the corresponding RDPS service over IPv4 or IPv6, as the case may be, will be considered as unavailable from that probe until it is time to make a new test. The minimum number of active testing probes to consider a measurement valid is ~~10~~20 at any given measurement period, otherwise the measurements will be discarded and will be considered inconclusive; during this situation no fault will be flagged against the SLRs.

Placement of RDPS probes. Probes for measuring RDPS parameters shall be placed inside the networks with the most users across the different geographic regions; care shall be taken not to deploy probes behind high propagation-delay links, such as satellite links. Every probe will have connectivity through multiple transit providers and rotate all RDPS tests through each provider in rotation. If a RDPS test fails through one transit provider the RDPS Probe will repeat the test in turn through all of the multiple transit providers and only register a failure if all transit providers fail. Each transit provider will represent a clear separate upstream network path divergent of the other transit providers.

Services between Contracted Parties:

EPP service availability. Refers to the ability of the TLD EPP servers as a group~~,~~ to respond to commands from the Registry accredited Registrars~~,~~ who already have credentials to the servers. The response shall include appropriate data from the Registry System. An EPP command with " **EPP command RTT**" 5-times higher than the corresponding SLR will be considered as unanswered. For the EPP service to be considered available ~~at~~ during a measurement period, at least, one IPv4 and one IPv6 (if EPP is offered over IPv6) address of the set of EPP servers must have defined results from "**EPP tests**". If ~~51% or more~~100% of the EPP testing probes see the EPP service as unavailable during a given time, the EPP service will be considered unavailable. The Registry Operator must notify Registrars of unplanned EPP service failure and provide updates no less than every 60 minutes until EPP service is restored. Registrars have the right to escalate EPP service failures that exceed the EPP Emergency Thresholds listed in Section 3 (see Section 6).

EPP session-command RTT. Refers to the **RTT** of the sequence of packets that includes the sending of a session command plus the reception of the EPP response for only one EPP session command. For the login command it will include packets needed for starting the TCP session. For the logout command it will include packets needed for closing the TCP session. EPP session commands are those described in section 2.9.1 of EPP RFC 5730. If the **RTT** is 5-times or more the corresponding SLR, the **RTT** will be considered undefined.

EPP query-command RTT. Refers to the **RTT** of the sequence of packets that includes the sending of a query command plus the reception of the EPP response for only one EPP query command. It does not include packets needed for the start ~~nor~~or close of ~~neither~~either the EPP ~~nor~~or the TCP session. EPP query commands are those described in section 2.9.2 of EPP RFC 5730. If the **RTT** is 5-times or more the corresponding SLR, the **RTT** will be considered undefined.

EPP transform-command RTT. Refers to the **RTT** of the sequence of packets that includes the sending of a transform command plus the reception of the EPP response for only one EPP transform command. It does not include packets needed for the start ~~nor~~or close of ~~neither~~either the EPP ~~nor~~or the TCP session. EPP transform commands are those described in section 2.9.3 of EPP RFC 5730. If the **RTT** is 5-times or more the corresponding SLR, the **RTT** will be considered undefined.

Measuring EPP parameters. Every 5 minutes, every EPP probe shall randomly select one "**IP address**" of the EPP servers of the TLD being monitored and make an "**EPP ~~tests~~**"; ~~every time it should randomly alternate between~~**test**" Each EPP test shall include the ~~3 different types of~~following commands as a set: an EPP session, EPP query and ~~between the commands inside each type for testing.~~EPP transform command . If an "**EPP test command**" gets unanswered, the relevant EPP service will be considered as unavailable from that probe until it is time to make a new test~~. The minimum number of active testing probes to consider a measurement valid is 10 at any given measurement period, otherwise the measurements will be discarded and will be considered inconclusive; during this situation no fault will be flagged against the SLRs~~.

Placement and Operation of EPP probes. Probes for measuring EPP parameters shall be placed ~~inside or close to Registrars points of access to~~ and operated by the ~~Internet across the different geographic regions; care shall be taken not to deploy probes behind high propagation delay links, such as satellite links.~~

~~**Listing of probes.** The current list of probes for DNS, RDPS and EPP can be consulted in <[redacted]>.~~ Registry Operator ~~is responsible to take the necessary steps to ensure that the listed probes do not get their tests blocked by its network equipment. The list can be updated~~inside all centers of operations from ~~time to time by ICANN provided it gives, at least, a 90 day notice to the~~where EPP Services are active to Registrars. Each Registry Operator ~~before making the change. During that period the Registry Operator,~~ will ~~have access to the readings for new probes and ICANN will not consider those measurements for SLA purposes.~~provide an annual inspection report, by an independent third party, to verify compliant operation of EPP monitoring probes with this agreement.

4.5 SLA Reporting

Principles for reporting on Public Services and Services between Contracted Parties:

Parties responsible for monitoring public services will produce weekly and monthly reports on service availability and SLA conformance. These reports will contain a single average of all tests,across all

applicable probes, or each monitored transaction type. Reports are not used for purposes of identifying emergencies or current outages. Reports are intended as lasting statements of record in regards to performance and SLA conformance, for tracking industry trends and for purposes of consumer transparency.

Public Service Monitoring:

Reports produced by ICANN with respect to Public Service Monitoring will be shared with the applicable Registry Operators in a joint review process. Reports will be submitted to the Registry Operator within one month of the end of the reporting period. Registry Operators will review and either agree or contest the result of the reporting within one month. Upon request, ICANN will provide any detailed monitoring data available in relation to the monitoring report in question so that the Registry Operator may reconcile reported results with their own findings. Registry Operators and ICANN must agree to the reporting results before said results can be posted for public consumption. Reports will be posted no earlier than three months from the closing of the reporting period.

Services between Contracted Parties:

Reports produced by Registry Operators with respect to monitoring services between Contracted Parties will be shared with ICANN in a joint review process. Reports will be submitted to ICANN within one month of the end of the reporting period. Upon request, Registry Operators will provide any detailed monitoring data available in relation to the monitoring report in question so that ICANN may reconcile reported results with their own records. Registry Operators and ICANN must agree to the reporting results before said results can be posted for public consumption. Reports will be posted no earlier than three months from the closing of the reporting period.

4.6 Emergency Escalations for Public Services, and Contracted Party Services

Principles of Emergency Escalation:

Escalations are strictly for purposes of notifying and investigating possible or potential issues in relation to monitored public services and monitored services between contracted parties. The initiation of any escalation and the subsequent cooperative investigations do not in themselves imply that a monitored service, public or between contracted parties, has failed availability or performance requirements.

Escalations shall be carried out between ICANN and Registry Operators, and Registrars and Registry Operators, only where there are 24 hour, 365 days a year available, emergency operations departments prepared to handle emergency requests. Registry Operators and ICANN must provide said emergency operations departments. Current contacts and escalation procedures must be agreed to and maintained between ICANN and Registry Operators and published to Registrars, where relevant to their role in escalations, prior to any processing of Emergency Escalations by all related parties, and kept current at all times.

Emergency Escalations regarding Public Services:

Upon reaching appropriate thresholds as described in Section 4 regarding Public Service monitoring, ICANN's emergency operations will initiate an Emergency Escalation with the relevant Registry Operator. An Emergency Escalation consists of the following minimum elements: both electronic (i.e., email or SMS) and voice contact notification to the Registry Operator's emergency operations department

with detailed information concerning the issue being escalated - including evidence of any and all monitoring failures, cooperative trouble-shooting of the monitoring failure between ICANN staff and the Registry Operator, and the commitment to begin the process of rectifying issues (as identified and agreed upon by both parties) with either the monitoring service or the service being monitoring.

Emergency Escalations regarding Services between Contracted Parties:

Registry Operators will maintain 24 hour, 365 days a year available, emergency operations departments prepared to handle emergency requests from Registrars. In the event that a Registrar is unable to conduct EPP transactions with the Registry because of a fault with the Registry Service and is unable to either contact (through ICANN mandated methods of communication) the Registry Operator, OR the Registry Operator is unable or unwilling to address the fault, the Registrar may initiate an Emergency Escalation to the emergency operations department of ICANN. ICANN will contact the Registry Operator through both electronic (i.e., email or SMS) and voice contact notification in order to confirm the Registry Operator is actively addressing the Registrar's inability to conduct EPP transactions. ICANN may, at that time, request relevant detailed monitoring data to confirm the availability of EPP services from the Registry Operator.

Notifications of Service Availability and Maintenance:

In the event that a Registry Operator plans maintenance, they will provide related notice to the ICANN emergency operations department 24 hours ahead of that maintenance. ICANN's emergency operations department will note planned maintenance times, and suspend Emergency Escalation services for related public, and contracted party, monitored services during the expected maintenance outage period.

If a Registry Operator declares an outage, as per their contractual obligations with ICANN, on services under SLA and performance requirements, they will notify the ICANN emergency operations department. During that declared outage, ICANN's emergency operations department will note and suspend emergency escalation services for related public, and contracted party, monitored services.

Appendix I: DNS Test Query and Response (Required Method)

Formatted: Font: Bold

Requirements and Setup

For each TLD, ICANN will require the registry to add the following to the TLD zone:

icanndnstestdomain.TLD. 0 IN DS <DS RDATA>

icanndnstestdomain.TLD. 0 IN RRSIG <RRSIG RDATA for the DS record>

icanndnstestdomain.TLD. 0 IN NS ns1.icanndnstestdomain.TLD.

icanndnstestdomain.TLD. 0 IN NS ns2.icanndnstestdomain.TLD.

ns1.icanndnstestdomain.TLD. 0 IN A <IPv4 address of ns1>

ns1.icanndnstestdomain.TLD. 0 IN A <IPv6 address of ns1>

ns2.icanndnstestdomain.TLD. 0 IN A <IPv4 address of ns2>

ns2.icanndnstestdomain.TLD. 0 IN A <IPv6 address of ns2>

The DS record (or DNSKEY record, if the registry uses DNSKEYs to generate their own DS records), Ipv4 and Ipv6 glue records will be provided by ICANN at a later date.

DNS Query #1: RTT calculation

The RTT query should return as consistent a result as possible across all TLDs. Because of this, DNSSEC data will not be included in this test (as the usage of different algorithms for signing may create different sized RRSIGs). As such, the query is defined as follows:

dig +nodnssec +norecurse +noall +auth +stat -t NS icanndnstestdomain.TLD. @<TLD_SERVICE_ADDRESS>

The expected response should look similar to the following:

icanndnstestdomain.TLD. 0 IN NS ns1.icanndnstestdomain.TLD.

icanndnstestdomain.TLD. 0 IN NS ns2.icanndnstestdomain.TLD.

;; Query time: 46 msec

;; SERVER: 199.254.31.1#53(199.254.31.1)

;; WHEN: Wed Feb 2 15:08:43 2011

;; MSG SIZE rcvd: 105

DNS Query #2: DNSSEC testing

For this test, the DS record (and its associated RRSIG will be queried. The response recieved will then be validated. Only TLDs that are signed and have valid DS records in the root zone will be tested in this manner.

The query for this test is defined as:

dig +dnssec +norecurse +noall +answer -t ds icanndnstestdomain.TLD. @<TLD_SERVICE_ADDRESS>

With an expected response similar to the following:

icanndnstestdomain.TLD. 0 IN DS 31129 5 1 91DE4126C0A6F37FFF43C7C5605793ECB79C68C1

icanndnstestdomain.TLD. 0 IN RRSIG DS 7 2 0 20110215155636 20110201145636 34260 org. KgJyKPSsLHwqrybWp1YbcsTImA2xwHrsp7c4ZBf5Qc8RIHBgwsugavZS OLlhOx8ms1ySD/tlh6NEP1Wg7Aci5XRDl5qqCiaxuEqf/MrY9h8lGsHg HfZP0C1JAWa+/nKqd7mtfN9QYd20r3WNcE/Wni54SC8KDgXGJlegXHqk xdM=

Note that the DS and RRSIG RDATA provided here is for illustrative purposes only, and is not the expected explicit output, since the DS and RRSIGS for this data is not yet generated.

Test Iterations

These tests will be conducted against each DNS Name Server for the TLD, as listed in the root zone at the time the test is conducted. Each test will be conducted using both UDP and TCP transports, and each transport will be tested over both Ipv4 and Ipv6 networks. This set of queries will collectively be referred to as the “DNS Test”.