RDS Purpose: Technical Issue Resolution
DT1 Answers to Questions – First Draft for DT Review

From latest Working Draft:
https://community.icann.org/download/attachments/79432604/KeyConceptsDeliberation-WorkingDraft-13Feb2018.pdf

> WG Agreement #46:
> Technical Issue Resolution for issues associated with Domain Name Resolution is a legitimate purpose, based on the following definition: *Information collected to enable contact of the relevant contacts to facilitate tracing, identification and resolution of incidents related to issues associated with domain name resolution by persons who are affected by such issues, or persons tasked (directly or indirectly) with the resolution of such issues on their behalf.*
>
> WG Agreement #47:
> The following information is to be collected for the purpose of Technical Issue Resolution associated with Domain Name Resolution:
> - Technical Contact(s) or (if no Technical Contact is provided) Registrant Contact(s),
> - Nameservers,
> - Domain Status,
> - Expiry Date and Time,
> - Sponsoring Registrar

Developed through deliberation on DT1 Output (November 2017):
https://community.icann.org/download/attachments/74580012/DT1%20-%20TechIssues-Research-final.pdf

1. ***Who associated with the domain name registration needs to be identified and/or contacted for the purpose of Technical Issue Resolution?***

Entities who observe or are affected by technical issues associated with a domain name need to contact domain contacts who are ~~the entities~~ tasked (directly or indirectly) with evaluating and solving such issues. These problems may include failure of services associated with the domain (such as email or a web site), failures or errors in DNS resolution, etc. Abuse often involved a technical issue, such as when phishing sites are placed on a compromised domain or malware infects the domain's server, and such cases are often approached and resolved via similar paths as service failures.

Comment [1]: The issue is not whether or not registrants may WISH to be contacted -- they often don't know there is a problem on their domain. Instead, the issue is that people observe problems and then need to reach out to the domain contacts. I've updated this paragraph accordingly.

The contacted party may be the domain name's ~~current "owner (the~~ Registrant (~~,~~ reached directly), the domain name's current user (the customer of a Privacy/Proxy provider, reached by relay through the PP), or a party designated by the Registrant as being tasked with resolution of technical issues associated with the domain name registration (i.e. an Administrative or Technical contact).~~.~~

For various legal and practical purposes, note that:

1. The Registrant is the party ultimately responsible for the domain name.
2. Some registrants have the resources to designate other parties who have responsibility or expertise to resolve the underlying problems. IN some cases registrars offer to act as teh Technical Contact for a domain,
3. In some cases the delegated contact may need the authorization of the Registrant in order to make a fix.

At the same time, ~~If the issue cannot be rectified via contact with the above partie~~s, the domain's sponsoring registrar ~~(the entity where the domain name is currently registered)~~ may also be contacted in an effort to reach affected parties. In some cases the sponsoring registrar is also the domain's hosting, DNS, and/or email provider. Outreach to the sponsoring registrar ~~For example, this may~~ may be also be necessary if the problem with domain name resolution interferes with successful email delivery to intended recipient. Contacting the sponsoring registrar in cases of security problems such as phishing attacks is also reasonable and practical, because such problems cause harm and are important to report and resolve in a as timely a fashion as possible.~~,~~ Outreach to registrars might increase under GDPR, which will reduce or eliminate the availability of domain contact data. Some parties performing outreach may not have the necessary knowledge to determine the hosting provider of a domain, but may be able to learn the registrar's identity via a WHOIS (RDS) query.

Question from WG call for DT to answer: Is the entity you want to reach for technical issue resolution sometimes or always the account holder because they have control over the domain name registration?

2. What is the objective achieved by identifying and/or contacting each of those entities?

The party initiating contact (e.g., abuse responder / reporter, IT professional, users of the domain name, or website operator) often has an interest in the issue being resolved (e.g., mitigating abuse, reestablishing connectivity or availability of systems and services associated with the domain name).

The entity being contacted for this purpose often wishes to be contacted for the same reasons and is benefitted. ~~In many cases, the entity (an individual or business) delegates responsibility for technical issue resolution to another entity with expertise needed to resolve the underlying problems (e.g., update nameservers, investigate the root cause for an unreachable website or mail server or compromised system).~~

Questions from WG call for DT consideration:

- *Is an objective having the ability to contact someone associated with the domain name registration who can quickly surmise and solve technical issues associated with the domain name such as botnets, email storms, etc?*
- *If an entity does wish to respond to contact attempts, that may be its prerogative, irrespective of the reason for the contact attempt. To the extent entities are not contactable, larger players may already know who to contact; they may or may note depend on WHOIS. Smaller players and outsiders will be impacted more if contact information is not provided through RDS. Privacy is important, but so is security and stability -- if we achieve privacy but break the internet, that is not a desirable outcome.*

3. What might be expected of that entity with regard to the domain name?

A domain contact will often have an obvious self-interest in fixing the issue.

The Internet is a connected system of networks and resources. Parties who control and operate such resources are generally expected to not allow the use of their resources in ways that allow harm to others.

The domain contact~~contacted entity~~ may or may not have an~~usually has no~~ legal obligation to respond to communication or to investigate the problem:~~.~~

RDS Purpose: Technical Issue Resolution
DT1 Answers to Questions – First Draft for DT Review

- A registrant may have an obligation depending upon what laws or legal obligations it is under. Examples include regulatory or breach notification laws;r contracts containing such obligations, including domain registration agreements; and contributory negligence liabilities.
- A proxy/privacy provider may have notification and communication obligations, per contracts and per forthcoming ICANN Consensus Policy (https://gnso.icann.org/en/issues/raa/ppsai-final-07dec15-en.pdf). Per the 2013 RAA, P/P Providers operated by registrars are required to publish "The circumstances under which the P/P Provider will relay communications from third parties to the P/P Customer" and "shall publish a point of contact for third parties wishing to report abuse".
- Per the 2013 RAA, gTLD registrars must maintain a dedicated abuse contact to receive reports of abuse involving Registered Names sponsored by Registrar, and Registrar shall publish on its website a description of its procedures for the receipt, handling, and tracking of abuse reports. Registrars must also "document its receipt of and response to all such reports."

When ~~However, when~~ a domain ~~t~~Technical C~~c~~ontact has been tasked with technical issue resolution, the registrant may expect the T~~t~~echnical C~~c~~ontact to have rights needed to update registration data associated with the domain name or systems using the domain name, and/or take actions that lead to resolution.

Question from WG call for DT to consider: Is the party making contact trying to alert the people managing the domain that they have a problem that would be to their benefit to resolve or is the party making contact trying to get attention to a problem that it has?

RDS Purpose: Academic or Public Interest DNS Research
DT1 Answers to Questions – First Draft for DT Review

From DT1 Output: https://community.icann.org/download/attachments/74580012/DT1%20-%20TechIssues-Research-final.pdf

> **Definition:** *Information collected to enable use of registration data elements by researchers and other similar persons, as a source for academic or other public interest studies or research, relating either solely or in part to the use of the DNS.*

1. ***Who associated with the domain name registration needs to be identified and/or contacted for the purpose of Academic or Public Interest DNS Research?***

Entities who buy/sell, register, or use domain names may benefit indirectly from academic or public interest DNS research.

The entities to be identified or contacted about each domain name registration (hereafter referred to as research subjects) depend upon the nature of the research, but may include the domain name's current owner (the Registrant), the domain name's current user (who may or may not be the customer of a Privacy/Proxy provider), a Privacy/Proxy provider associated with the domain name, or the Registrar of record associated with the domain name.

Identification of research subjects is often not strictly necessary for this purpose; for example, research that is performed through aggregation of domain name characteristics obtained from registration data, without regard to registrant or registrar. However, for research tasks such as determining a domain name's registration history, identifying the past and present entities associated with a specific domain name may be essential to the study.

Contact with each entity for research purposes may not be necessary or desired by those entities. For example, the GNSO-sponsored study of WHOIS abuse included surveying registrants about their experiences with abuse of contact data published in WHOIS – this study was performed for the indirect benefit of all entities with contact data in WHOIS. However, some entities may view unsolicited survey invitations as intrusive or perceive contactability for research as a risk not benefit.

2. ***What is the objective achieved by identifying and/or contacting each of those entities?***

The party initiating contact (e.g., Internet researcher, ICANN, government) has an interest in performing the study (e.g., cybercrime research, WHOIS accuracy studies, Internet proliferation studies, legal and economic analysis of the DNS or domain name registration systems, research to inform public policy). As such, that party benefits directly from access to WHOIS data for this purpose, including data associated with the research subject or domain name that may not be personally-identifiable information (e.g., country of the registrant, sponsoring registrar).

The entity being identified or contacted for this purpose may not directly benefit, but may indirectly benefit through reduction in cybercrime, improvements in public policy, fewer data inaccuracies, Internet capacity building, enforcement of laws, consumer protection, etc. Benefits to the research subject depend upon the nature of the research.

In some cases, the research subject may benefit directly – for example, if a prospective buyer is researching the history of a domain name before purchasing it from a willing and interested seller.

3. What might be expected of that entity with regard to the domain name?

The identified or contacted entity has no obligation to respond to communication initiated for academic or public interest DNS research.

RDS WG – Drafting Team 2: Domain Name Management and Individual Internet User

Purpose Name: **Domain Name Management**

WG Agreement 48:
Domain Name Management is a legitimate purpose for collecting some registration data, based on the definition: Information collected to create a domain name registration, enabling management of the domain name registration, and ensuring that the domain registration records are under the control of the authorized party and that no unauthorized changes or transfers are made in the record.

WG Agreement 49:
The following information is to be collected for the purpose of Domain Name Management:

- Domain Name
- Registrant Name
- Registrant Organization
- Registrant Email
- Registrar Name
- Creation Date
- Updated Date
- Expiration Date
- Nameservers
- Domain Status
- Administrative Contact

From https://community.icann.org/download/attachments/79432604/KeyConceptsDeliberation-WorkingDraft-13Feb2018.pdf
Note that WG Agreements 48 and 49 were inserted above, as they supersede DT2's original definition of this purpose.

ICANN 61 Questions and Answers

1. Who associated with the domain name registration needs to be identified and/or contacted for each purpose?

The entity identified in this use case is the individual (either private or associated by an organization) who has made the decision to purchase the domain name in order to provide access to Internet services that are or will be made available using the domain name.

This individual has the ultimate say in not only how the domain name is used but is responsible for the domain name management functions including resolving (or knowing how to resolve) operational issues, handling issues related to legal actions, care and update of WHOIS contact details (including ICANN contractual issue), and the ultimate sale and transfer of the domain name.

The entity or entities that need to be identified and respond vary depending on the registration. A simple/personal domain name registration may involve a single entity that is

responsible for all aspects of the domain. Large corporate domain name registration may involve numerous entities each responsible for a specific area.

Specifically

- Selection and creation of the Domain Name – Registrant
- Creation of registrant ID – Registrar
- Configuration of DNS Data (Nameserver IP): Registrant or Organizational DNS Administrator.
- Monitoring and maintenance of WHOIS Status data – Registry and Registrar
- Monitoring to ensure Nameserver and registration data is correct/authoritative – Registrar, Registry, "Tech Contact", "Admin Contact".

2. What is the objective achieved by identifying and/or contacting each of those entities?

The purchase [?] and use of a domain name comes with various responsibilities, mostly related to the ensuring the domain name properly resolves and the services associated with the name (and IP) are operational and are being used for indented purposes.

The main objective to identify and to contact this individual is to ensure the ability to address the management related items listed in "Tasks" above, [including who is adding/removing data].

3. What might be expected of that entity with regard to the domain name?

Expectations include the ability to respond and act authoritatively [and responsively] with issues related to registration, issue resolution, domain name transfer, and issues related to legal actions. This entity should also have the ability to determine [after the fact] why changes to domain name data were allowed.

Purpose Name: **Individual Internet User**

Definition: Collecting the required information of the registrant or relevant contact in the record to allow the internet user to contact or determine reputation of the domain name registration.

From https://community.icann.org/download/attachments/74580010/RDS%20WG%20DT2%20Draft%20edits%201113.pdf

Note that a link to DT2's previously-published output for this purpose was inserted above.

ICANN 61 Questions and Answers

1. Who associated with the domain name registration needs to be identified and/or contacted for each purpose?

The entity identified in this use case is the individual (either private or associated with an organization) who has made the decision to purchase the domain name and has ultimate responsibility for the in order to provide access to Internet services that are or will be made available using the domain name.

2. What is the objective achieved by identifying and/or contacting each of those entities?

The objective for Internet end users is to easily identify the domain name Owner in order to determine if its safe to complete a commercial transaction using a service associated with the domain name.

In the case of technical issue resolution the objective is to ensure the ability to contact registrant in case of operational issues related to domain name resolution and services associated with the domain name (e.g. ability to identify ISP/Hosting provider).

3. What might be expected of that entity with regard to the domain name?

Expectations include the ability to properly identify the domain name owner and solve/address operational issues including problems related to abuse and the ability be informed of possible consequences.,.

[Gnso-rds-pdp-3] [EXTERNAL] Reconvening Domain Name Certification team

David Cake dave at davecake.net
Mon Mar 5 17:59:05 UTC 2018

- Next message: [Gnso-rds-pdp-3] [EXTERNAL] Reconvening Domain Name Certification team
- **Messages sorted by:** [date] [thread] [subject] [author]

I think we should divide our answer according to the type of certificate required. The request from the leadership is that we add clarifying information even if it does not currently require the RDS.

Anyone objet to any of the below?

For all certificates, including domain name certificates.
- the person who need to be identified is a person who controls the domain name.
- the objective achieved is proof that the request for the certificate originates from someone with control over the domain name.
- this may be achieved by multiple methods, some of which use some elements of the RDS, some of which use the DNS, some of which use non-technical means. The means that do use the RDS may use email, fax, SMS, postal mail or phone numbers, as described in the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates 3.2.2.4.2 and 3.2.2.4.3

I also note that for the method of Domain contact verification via a Domain Authorisation Document, verification that WHOIS data has not changed is required, but this method is not to be used after August 2018. We recommend this method is ignored for purpose of working group deliberation for that reason.

For an Extended Validation certificate:
- Four roles are possibly needed for an Extended Validation certificate to be issues, an authorized Certificate Requester, authorized Certificate Approver, an authorized Contract Signer, and an authorized Applicant Representative
 These are natural persons who are either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant for that role (they may be a single person). These roles must be validated by independent means to the RDS.
- the Drafting team believes these roles, and other aspects of Extended Validation apart from the demonstrating control of the domain name, do not depend on the RDS or DNS, and so are outside the scope of the work on this working group.

> *On 28 Feb 2018, at 8:25 am, Feher, Kal <Kalman.Feher at team.neustar> wrote:*
>
> *Hello David and fellow certifiable team members,*
> *I've had a very relaxing 3 week vacation, so I'm a little behind, but I've read through the instructions so I'll make some suggestions.*
>
> *Firstly before I comment on the open questions I'd like to make an observation based on the feedback and comments we received when presenting our prior findings. Depending on their perspectives and experience, many WG members did not truly understand that we had restricted our scope to the use of registration data in the work flow of obtaining a certificate (from a CA) for a domain name. We'd also strictly followed the documented workflow agreed to by the CA/Browser forum. No independent or alternate certificate allocation workflows were considered. It is my opinion that the narrow scoping was appropriate then and remains so now. However it may be required that we continue to clarify this point in any submission we make to the WG.*
>
> *Here's some thoughts on the questions:*

> Bearing in mind that the only purpose registration data is used in the CA/Browser forum guidelines is for proof of domain control.
>
> --=Who associated with the domain name registration needs to be identified and/or contacted for this purpose?=--
> Someone who controls the domain name. A contact filling a technical or administrative role would seem to be the most appropriate. Note that direct contact is not strictly required to deliver proof of domain control and remains a single option amongst many alternatives for such proof. Therefore the answer to this question could also quite legitimately be "no one needs to be identified and/or contacted for this purpose".
>
> --=What is the objective achieved by identifying and contacting each of those entities?=--
> Proof that the request for the certificate is supported by an entity that has control of the the domain in question.
>
> --=What might be expected with regard to that domain name?=--
> I have nothing to add here.
>
> --
> Kal Feher
> Neustar Inc.
> Melbourne, Australia
>
>
> From: Gnso-rds-pdp-3 <gnso-rds-pdp-3-bounces at icann.org <mailto:gnso-rds-pdp-3-bounces at icann.org>> on behalf of David Cake <dave at davecake.net <mailto:dave at davecake.net>>
> Date: Wednesday, 28 February 2018 at 08:57
> To: "gnso-rds-pdp-3 at icann.org <mailto:gnso-rds-pdp-3 at icann.org>" <gnso-rds-pdp-3 at icann.org <mailto:gnso-rds-pdp-3 at icann.org>>
> Subject: [EXTERNAL] [Gnso-rds-pdp-3] Reconvening Domain Name Certification team
>
> If you were on the call earlier, you would have heard that the leadership of the Next Generation RDS PDP WG have decided to reconvene the separate Drafting Teams, including the team for Domain Name Certification. We would like to take a week to prepare for discussion at the face to face meeting at iCANN 61.
>
> We would like to reopen discussion, and the new questions we would like the team to answer are:
>
> Who associated with the domain name registration needs to be identified and/or contacted for this purpose?
> What is the objective achieved by identifying and contacting each of those entities?
> What might be expected with regard to that domain name?
>
> All the teams are requested to not restrict themselves to existing data elements, but try to answer the questions conceptually and explicitly.
>
> To prep for ICANN61, it is imperative that we discuss these questions and produce output over the next week – ideally by 5 March but no later than 7 March.
>
> We know this is a short timeframe.
>
> To learn more about this assignment, please read these instructions:
>
https://community.icann.org/download/attachments/79432608/Drafting%20Team%20Assignment%2026%20Feb.pdf <https://community.icann.org/download/attachments/79432608/Drafting%20Team%20Assignment%2026%20Feb.pdf>

>
> If you did not attend today's WG call, you can catch up by reading or listening to the call recording/notes/transcript:
> https://community.icann.org/x/oAu8B <https://community.icann.org/x/oAu8B>
>
> We need to get started immediately – within 24 hours ideally. We may also be having some new volunteers join the team.
>
> David

>

-------------- next part --------------
An HTML attachment was scrubbed...
URL: <http://mm.icann.org/pipermail/gnso-rds-pdp-3/attachments/20180306/ea7ca464/attachment.html>
-------------- next part --------------
A non-text attachment was scrubbed...
Name: signature.asc
Type: application/pgp-signature
Size: 488 bytes
Desc: Message signed with OpenPGP
URL: <http://mm.icann.org/pipermail/gnso-rds-pdp-3/attachments/20180306/ea7ca464/signature.asc>

- Next message: [Gnso-rds-pdp-3] [EXTERNAL] Reconvening Domain Name Certification team
- **Messages sorted by:** [date] [thread] [subject] [author]

More information about the Gnso-rds-pdp-3 mailing list

RDS Purpose: Domain Name Purchase/Sale
DT4 Answers to Questions – Final 7 March 2018

From https://community.icann.org/download/attachments/74580010/DraftingTeam4-DNPurchaseSale-Purpose-v9-clean.pdf

> Purpose Summary: Information to enable contact between the registrant and third-party buyer to assist registrant in proving and exercising property interest in the domain name and third-party buyer in confirming the registrant's property interest and related merchantability.
>
> Definition: This purpose enables contact between domain name registrants and third-party buyers (e.g., small business owners, corporations, and domain name brokers) for unsolicited domain name purchase queries, and for both parties to complete and confirm agreed domain name transfers from seller to buyer.

1. Who associated with the domain name registration needs to be identified and/or contacted for each purpose?

Third-party buyers (e.g., small business owners, corporations, and domain name brokers) need to identify the person or entity that currently holds the rights to a domain name being purchased.

This party may be the domain name's current owner (the Registrant, reached directly) or the domain name's current user (the customer of a Privacy/Proxy provider, reached by relay through the PP).

Buyers may also need to identify persons or entities that have previously held the rights to a domain name being purchased, to assess the domain name's merchantability.

2. What is the objective achieved by identifying and/or contacting each of those entities?

Prior to acquisition, buyers use contact information to send purchase inquiries, in hopes of finding someone willing to sell the desired domain name.

During due diligence, buyers need to identify the party who currently holds the rights to a domain name, confirm whether that potential seller has a relationship with the Registrant Organization, and identify other domain names with which the buyers or sellers may be associated.

To complete a domain name acquisition, buyers need to identify the old and new Registrant to verify that the domain name change in ownership has been accurately recorded.

3. What might be expected of that entity with regard to the domain name?

The potential seller may prefer not to be contacted for this purpose and is under no obligation to reply to such solicitations. In some jurisdictions, unsolicited solicitations may be considered spam, and repeated "offers to buy" can be construed as harassment.

The buyer expects that the Registrant (or for Privacy/Proxy-registered domain names, the PP customer) has the legal right to sell the domain name.

In the case of relayed communication, both buyer and seller expect communication to the authentic entity who has legal rights to sell the domain name to be relayed by the Privacy/Proxy. [1]

Once the seller initiates transfer of the domain name to the buyer, the registrar is expected to complete the transfer process.[1]

Additional steps, checks, and processes may need to take place depending on the terms of purchase/sale – this is commonly but not only when additional parties. For example, if an escrow agent is involved, they are expected to verify the transfer to buyer before releasing funds.

[1] The rights and duties of the registrar, the PP, and the registered name holder are detailed in contracts between those parties.

RDS Purpose: ICANN Contractual Enforcement

DT5 Answers to Questions – Final Version for WG Review 7 March 18

From: https://community.icann.org/display/gTLDRDS/Phase+1+Documents (See the 2nd link for DT5)

Definition: Information accessed to enable ICANN Compliance to monitor and enforce contracted parties' agreements with ICANN.

1. *Who associated with the domain name registration needs to be identified and/or contacted for the ICANN Contractual Enforcement Purpose?*

    - ICANN compliance needs to be able to identify and as necessary contact the representatives from the associated registrar and/or registry who is knowledgeable about the contracted party's fulfillment of RDS or other contractual requirements. ICANN compliance may also need to contact the registrant or its designated representative to confirm or verify facts or assertions made regarding the registrar's or registry's compliance.

2. *What is the objective achieved by identifying and/or contacting each of those entities?*
    - The objectives for contacting any of the entities listed for question 1 above, if needed, are:
        - To provide notification of any possible compliance issues
        - To ask clarifying questions about any possible compliance issues
        - To communicate possible compliance actions under consideration
        - To provide official notification of final actions taken.

3. *What might be expected of that entity with regard to the domain name?*
    - Domain name registrars and registries would be expected (by ICANN compliance) to do any or all the following as applicable:
        - Ask clarifying questions about issues identified by ICANN Compliance
        - Respond to questions asked by ICANN Compliance
        - Provide relevant information to assist ICANN Compliance in their deliberation.
        - Appeal actions taken by the ICANN Compliance.

Comment [O1]: It is important to note that there was divergence in the DT about whether ICANN Compliance would need to contact registrants in fulfilling its responsibilities. The DT reached out to Compliance to seek their input.

Comment [O2]: It may be helpful to understand that some contract requirements relate directly to the RDS. In its deliberation going forward on the proposed purpose of ICANN Contractual Enforcement, the WG may need to decide whether this purpose should just involve RDS related contractual requirements or compliance with all contract requirements.

RDS Purpose: Regulatory

DT5 Answers to Questions – Final Draft for WG Review - 7 Mar 18

From: https://community.icann.org/display/gTLDRDS/Phase+1+Documents (See the 1st link for DT5)

Definition: Information accessed by regulatory entities to enable contact with the registrant to ensure compliance with applicable laws.

1. *Who associated with the domain name registration needs to be identified or contacted for the proposed Regulatory Purpose?*
   - Applicable regulatory authorities with potential jurisdiction over the registrant, registrar and registry may need to be able to identify and as necessary contact the following:
     a. The domain name registrant or designated representative
     b. The domain name registrar
     c. The domain name registry.

2. *What is the objective achieved by identifying and/or contacting each of those entities?*
   - The objectives of identifying any of the entities listed for question 1 above are:
     - For a: to determine who is the authorized holder of the domain name registration and what is that entity's legal jurisdiction.
     - For b: to determine what registrar entered the domain name into the applicable top-level domain registry and what is the registrar's legal jurisdiction.
     - For c: to determine what registry entered the domain name into its top-level domain registry and what is the registry's legal jurisdiction.
   - The objectives for contacting any of the entities listed for question 1 above, if needed, are:
     - To provide notification of any possible regulatory issues
     - To ask clarifying questions about any possible regulatory issues
     - To communicate possible regulatory actions under consideration
     - To provide official notification of final actions taken.

3. *What might be expected of that entity with regard to the domain name?*
   - Domain name registrants or designated representatives could do any or all the following as applicable:
     - Confirm they are the authorized holder of the domain name registration
     - Identify their legal jurisdiction
     - Ask clarifying questions about issues identified by the regulatory agency
     - Respond to questions asked by the regulatory agency

Comment [O1]: Note that one DT member objected to asking this question because that member believes ICANN is not a regulator.

Comment [O2]: Note that the drafting team did not assume that public identification of any of the three entities is required.

Comment [O3]: One DT member said that this should be deleted because ICANN is not a law enforcement agency nor is it a customer protection agency.

Comment [O4]: If a is deleted in Q1 above, it should be deleted here.

Comment [O5]: One DT member said that all of these should be deleted because they are outside the clarity, scope, definition and strict boundaries of a "purpose" statement. (It should be noted that this is not a purpose statement.)

Comment [O6]: Note that a registrant, while subject to the terms and conditions of its contract with a registrar, may take any action it likes. Once the requesting entity has the contact info for a registrant, the registrant's behavior or action is not the concern of the registrar or registry unless the regulatory authority makes a legal request for action from the registrar or registry (e.g., server hold).

Comment [O7]: One DT member suggested inserting the following before 'could . . .': " if contacted by or through the registry or registrar from whom they receive the domain name".

- Provide relevant information to assist the regulatory agency in their deliberation.
- Appeal actions taken by the regulatory agency.

- Domain name registrars could do any or all the following as applicable:
  - Confirm they are the registrar of the domain name registration
  - Identify their legal jurisdiction
  - Ask clarifying questions about issues identified by the regulatory agency
  - Respond to questions asked by the regulatory agency
  - Provide relevant information to assist the regulatory agency or ICANN in their deliberation.
  - Put the regulatory agency, as legal and appropriate, in touch with the registrant.
  - Appeal actions taken by the regulatory agency.
- Domain name registries could do any or all the following as applicable:
  - Confirm they are the registry of the domain name registration
  - Identify their legal jurisdiction
  - Ask clarifying questions about issues identified by the regulatory agency
  - Respond to questions asked by the regulatory agency
  - Put the regulatory agency, as legal and appropriate, in touch with the registrant.
  - Provide relevant information to assist the regulatory agency in their deliberation
  - Appeal actions taken by the regulatory agency.

Comment [O8]: Note that registries can set their own internal policies with regard to how they respond to LEAs, or other regulatory requests, as appropriate to how the request is made and jurisdictional requirement.

RDS Purpose: Legal Actions

DT6 Answers to Questions – 3rd Draft for DT Review 5 Mar 18

From:
file:///C:/Users/Owner/Downloads/DT6%20Deliverable%20for%20the%20Legal%20Actions%20Purpose%20(Use%20Case)%20-%208%20Nov%20171.pdf

Definition: The "legal actions" purpose of RDS includes assisting certain parties(or their legal representatives, agents or service providers) to investigate and enforce civil and criminal laws, protect recognized legal rights, address online abuse or contractual compliance matters, or to assist parties defending against these kinds of activities, in each case with respect to all stages associated with such activities, including: investigative stages; communications with registrants, registration authorities or hosting providers, or administrative or technical personnel relevant to the domain at issue; arbitrations; administrative proceedings; civil litigations (private or public); and criminal prosecutions.

1. *Who associated with the domain name registration needs to be identified and/or contacted for each purpose?*

- To determine if a legal action may be warranted, legal entities may need to identify and possibly contact one or more of the following:
  a. The person or entity that currently owns the rights to the domain name or the rights holder's designated representative; this could be the registrant or the domain name's current user as in the case of a privacy or proxy service via a relay service.
  b. The registrar and/or reseller with whom the rights holder has a registration agreement for the domain name.
  c. The domain name registry for the associated top-level domain.
  d. Operator of domain name server(s)

Comment [O1]: Note that the operator of the domain name server(s) is not a currently collected data element for Whois. But name servers are collected and they can possibly be used to identify the operator of the servers.

2. *What is the objective achieved by identifying and/or contacting each of those entities?*

- The objectives of identifying any of the entities listed for question 1 above are:
  - For a: to determine who is the authorized holder of the domain name registration and what is that entity's legal jurisdiction.
  - For b: to determine what registrar entered the domain name into the applicable top-level domain registry and what is the registrar's legal jurisdiction.
  - For c: to determine what registry entered the domain name into its top-level domain registry and what is the registry's legal jurisdiction.

    - For d: if possible, to determine the identity of the web hosting provider associated with any content located at the domain name and what is the hosting provider's jurisdiction
- The objectives for contacting any of the entities listed for question 1 above, if needed, are:
    - For a: To provide notification of any possible legal issues affecting the authorized holder of the registration and to confirm legal jurisdiction
    - For b: To ask clarifying questions about any possible legal issues and to confirm the registrar's legal jurisdiction
    - For c: To ask clarifying questions about any possible legal issues and to confirm the registry's legal jurisdiction
    - For d: If possible, to ask clarifying questions about any possible legal issues and to confirm the hosting provider's legal jurisdiction
    - For a, b, c & d as applicable:
        - To communicate possible legal actions under consideration such as but not limited to cancelling the domain registration, transferring the domain name or removing website content associated with the name
        - To provide official notification of final actions taken.

3. *What might be expected of that entity with regard to the domain name?*

- Domain name registrants or designated representatives would be expected to do any or all the following as applicable in response to requests from legal authorities:
    - Confirm they are the authorized holder of the domain name registration
    - Identify their legal jurisdiction
    - Ask clarifying questions about issues identified by the legal authority
    - Respond to questions asked by the legal authority
    - Provide relevant information to assist the legal authority in their deliberation
    - Take other specific actions as requested or directed by the legal authority" for each of the categories
    - Appeal actions taken by the legal authority.
- Domain name registrars would be expected to do any or all the following as applicable in response to requests from legal authorities:
    - Confirm they are the registrar of the domain name registration
    - Identify their legal jurisdiction
    - Ask clarifying questions about issues identified by the legal authority
    - Respond to questions asked by the legal authority
    - Provide relevant information to assist the legal authority in their deliberation
    - Appeal actions taken by the legal authority.
- Domain name registries would be expected to do any or all the following as applicable in response to requests from legal authorities:
    - Confirm they are the registry of the domain name registration
    - Identify their legal jurisdiction

    - Ask clarifying questions about issues identified by the legal authority
    - Respond to questions asked by the legal authority
    - Provide relevant information to assist the legal authority in their deliberation
    - Appeal actions taken by the legal authority.
- Domain name registrants (or designated representatives), registrars or registries would be expected to respond at their discretion to communications from entities seeking civil or prior to litigation relief. Respond doesn't mean to comply with the request, but rather acknowledge the request and let the requestor know what action, if any, will be taken.

RDS Purpose: Criminal Activity or DNS Abuse Mitigation
DT7 Answers to Questions – First Draft for DT Review

Criminal Activity/ DNS Abuse Mitigation

Definition: The broad category of criminal activity or DNS abuse mitigation covers all use of an RDS to support criminal and other investigations, abuse prevention, security incident response, and other activities to protect people, systems, and networks from detrimental activities. These activities range from criminal activities like extortion, phishing, and provision of child abuse materials to abusive activities including denial-of-service attacks, spam, and harassment.

Criminal Activity/DNS Abuse Mitigation – Investigation

From https://community.icann.org/download/attachments/74580010/DraftingTeam7-CrimInvAbuseMit-10%20Nov%202017%20clean.pdf?version=1&modificationDate=1510442602000&api=v2

> Purpose Summary: The following information is to be made available to regulatory authorities, law enforcement, cybersecurity professionals, IT administrators, automated protection systems and other incident responders for the purpose of enabling identification of the nature of the registration and operation of a domain name linked to abuse and/or criminal activities to facilitate the eventual mitigation and resolution of the abuse identified: Domain metadata (registrar, registration date, nameservers, etc.), Registrant contact information, Registrar contact Information, DNS contact, etc..

1. ***Who associated with the domain name registration needs to be identified and/or contacted for investigation of Criminal Activity/DNS Abuse?***

During investigation of Criminal Activity/DNS Abuse, users of registration data, such as regulatory authorities, law enforcement, cybersecurity professionals, IT administrators, automated protection systems and other incident responders, may wish to identify the entity or individual who is in control of the domain name registration or who can provide information that would lead to the identification of the entity or individual who is controlling the domain name registration. Generally, this use case isn't for contact but is focused instead on identification. Accurate RDS data is important and can be critical in determining if the registrant is a victim of abuse or the abuser. While accurate data is preferred even bad data can be useful in identifying trends, showing patterns or association with known bad actors.

2. ***What is the objective achieved by identifying and/or contacting each of those entities?***

Identification of the entity responsible for criminal activity could lead to prosecution. The RDS data may be used in conjunction with other data points to build a case. As previously noted even bad data can be useful and may help demonstrate patterns or trends of abuse.

The objectives are:

1) Prevention of criminal activity and DNS abuse
2) Mitigation of impacts from criminal activity and DNS abuse
3) When it does occur providing data points to help build a case for prosecution of those responsible for the criminal activity

This use case generally uses the RDS data for identification but not for contact. In cases where a reseller or privacy/proxy service is used however, then contact with the objective of identifying domain owner (for purposes specified above) applies.

3. What might be expected of that entity with regard to the domain name?

If the entity or individual who is in control of the domain name registration cannot be identified, the party with access to that information (e.g. the privacy/proxy service or registrar) is expected to provide information concerning the entity or individual who is in control of the domain name registration so that the investigation can establish what role the entity or individual played in the DNS abuse and further abuse can be mitigated.

If the entity can be identified, it is expected that the entity will either want to be notified of and mitigate any associated crime/abuse, or the entity is the abuser and subject to further investigation.

RDS Purpose: Criminal Activity or DNS Abuse Mitigation
DT7 Answers to Questions – First Draft for DT Review

Criminal Activity/DNS Abuse Mitigation – Notification

From https://community.icann.org/download/attachments/74580010/DraftingTeam7-CrimInvAbuseMit-10%20Nov%202017%20clean.pdf?version=1&modificationDate=1510442602000&api=v2

> Purpose Summary: The following information is collected and made available for the purpose of enabling notification by regulatory authorities, law enforcement, cybersecurity professionals, IT administrators, automated protection systems and other incident responders of the appropriate party (registrant, providers of associated services, registrar, etc), of abuse linked to a certain domain name registration to facilitate the mitigation and resolution of the abuse identified: Registrant contact information, Registrar contact Information, DNS contact, etc..

1. ***Who associated with the domain name registration needs to be identified and/or contacted for Notification of Criminal Activity/DNS Abuse?***

During Notification of Criminal Activity/DNS Abuse, users of registration data, such as regulatory authorities, law enforcement, cybersecurity professionals, IT administrators, automated protection systems and other incident responders, may need to contact the entity or individual who is in control of the domain name registration or who can provide information that would lead to notification of the entity or individual who is controlling the domain name registration. This entity could be the domain name registration holder (the Registrant), the privacy/proxy service and/or the registrar. This is often an entity being harmed by Criminal Activity or DNS Abuse associated with a domain name – for example, when a domain name has been hijacked or compromised. The who may be another entity associated with the domain name registration (e.g., registrar, proxy) that can help notify the harmed entity. The who in this use case is often the victim of criminal activity or DNS abuse and needs to be someone authoritative for the domain who if necessary can take corrective action to mitigate or stop the abusive activity.

2. ***What is the objective achieved by identifying and/or contacting each of those entities?***

In some cases, the victim may not be aware of any issues, so the primary objective is notification of the problem. The secondary objective is that by notifying the appropriate party of an issue it can be corrected or otherwise mitigated. Enabling notification of the appropriate party (registrant, providers of associated services, registrar, etc), of crime or DNS abuse linked to a certain domain name registration is intended to facilitate the mitigation and resolution of the crime/abuse identified. Mitigation of criminal activity or DNS abuse associated with domain names is essential to promote the security and stability of the Internet, and thus of potential benefit to both victims of crime/abuse and indirectly to all Internet users.

3. ***What might be expected of that entity with regard to the domain name?***

Following notification, the entity in control of the domain name registration is expected to mitigate and resolve the abuse identified. In some instances, action might be expected of an entity other than the owner of the domain name registration. For example, when notified of certain types of abuse, a registrar might be expected to take down a domain name registration or otherwise prevent it from resolving.

RDS Purpose: Criminal Activity or DNS Abuse Mitigation
DT7 Answers to Questions – First Draft for DT Review

Criminal Activity/DNS Abuse – Reputation

From https://community.icann.org/download/attachments/74580010/DraftingTeam7-CrimInvAbuseMit-10%20Nov%202017%20clean.pdf?version=1&modificationDate=1510442602000&api=v2

> Purpose Summary: The following information is to be made available to organizations running automated protection systems for the purpose of enabling the establishment of reputation for a domain name to facilitate the provision of services and acceptance of communications from the domain name examined: Domain metadata (registrar, registration date, nameservers, etc.), Registrant contact information, Registrar contact Information, DNS contact, etc..

1. ***Who associated with the domain name registration needs to be identified and/or contacted for Reputation Analysis associated with Criminal Activity/DNS Abuse Mitigation?***

During reputation analysis to mitigate Criminal Activity/DNS Abuse, various data points are used to determine a reputation score. Who is but one of the elements that may be used by the scoring algorithm. Data needed will typically be those attributes that tend to cluster for abusive domain names including nameservers, registrar, creation date, registrant contact info (particularly e-mail, phone, and name), other contact information.

2. ***What is the objective achieved by identifying and/or contacting each of those entities?***

Enabling the establishment of reputation for a domain name to facilitate the provision of services and acceptance of communications from the domain name examined.

A company might make use of a reputation service to determine whether to allow traffic to a site. The objective here would be to protect users of the reputation service from Criminal Activity / DNS Abuse.

3. ***What might be expected of that entity with regard to the domain name?***

No contact would be expected for this use case; however, a domain name owner might be expected to provide accurate and up to date information if he/she is motivated to obtain a higher reputation score.