Template for defining an RDS Purpose:
Technical Issue Resolution -and- Academic or Public Interest DNS Research

Technical Issue Resolution
Academic or Public Interest DNS Research

Mailing list address: gnso-rds-pdp-1@icann.org
Mailing list archive: http://mm.icann.org/pipermail/gnso-rds-pdp-1/
Coordinated by: Michele Neylon
Members: Greg Aaron, Alan Woods, Greg Shatan, Stephanie Perrin, Jonathan Matkowsky, Nathalie Coupet, James Galvin

Template for defining an RDS Purpose:
Technical Issue Resolution -and- Academic or Public Interest DNS Research

Purpose Name: **Technical Issue Resolution**

Definition: *Information collected to enable contact of the relevant contacts to facilitate tracing, identification and resolution of incidents related to services associated with the domain name by persons who are affected by such issues, or persons tasked (directly or indirectly) with the resolution of such issues on their behalf.*

User	Purpose	Example Use Cases	Rationale for registration data access
Internet users affected by technical issues or those tasked with technical issue resolution on their behalf	Technical Issue Resolution	Contact to resolve problems with website, hosting, email service, etc.	Facilitate contact with domain contact (individual, role or entity) who can help resolve technical or operational issues with Domain Name (e.g., DNS resolution failures, email delivery issues, website functional issues, compromised hosting)

Tasks:.

- Compromised hosting
- Email not working / Issue with mail servers
- Identifying the hosting provider / registrar
- Problem with DNS hosting - e.g. you can't access a website (name doesn't resolve) - nameservers not responding.
- Website offline

NOTE: resolving technical issues often involves data associated with multiple domain names, e,g., domain, mail domain, nameserver domain, specific service used domain.

Data:

- Technical Contacts (whoever they may be)

- Registrant contacts
- Nameservers
- Server Status
- Expiry data

Sample Users:

- Abuse responder / reporter
- IT professionals
- Internet users (for the purposes of reporting an issue to the domain / website operator?)

Template for defining an RDS Purpose:
Technical Issue Resolution -and- Academic or Public Interest DNS Research

Purpose Name: **Academic or Public Interest DNS Research**

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.***

Tasks:

- Location / name of registrar is used by ICANN and others in reports around market penetration, usage and other metrics
- Identifying trends or patterns in domain registration, e.g., domains associated with a particular topic or event
- Demographics
- Lifecycle research
- EPP statuses
- Abuse related research

Data:

- Registrar of record
- Nameservers
- domain name string or substring
- Registrant details
- All fields really

User	Purpose	Example Use Cases	Rationale for registration data access
Internet Researchers	Academic or Public Interest	Domain Name Registration History	Enable historical research about a domain name registration (WhoWas)

Template for defining an RDS Purpose:
Technical Issue Resolution -and- Academic or Public Interest DNS Research

	DNS Research	Domain Names for Specified Contact	Enable identification of all domains registered with a given name, address, nameserver, registration date, etc. (Reverse Query)
		Survey Domain Name Registrant or Designated Contact	Enable surveys of domain name Registrants or their designated contacts
Internet Researchers	Academic or Public Interest DNS Research	Cybercrime research	Understand patterns of registration, hosting, methods used by cybercriminals. See also Domain Name Registration History and Domain Names for Specified Contact above.
Internet Researchers, ICANN	Academic or Public Interest DNS Research	WHOIS accuracy studies	ICANN contractual enforcement. Cybercrime research.
Internet researchers, governments	Public policy research	Studies of Internet proliferation	Capacity-building. ICANN mission. Requires examination of domain contacts.
Internet researchers, governments	Public policy research	Legal and economic analysis	Determine need for and effect of laws (e.g., GDPR) on data accessibility, on privacy, on registry and registrar practices, on stakeholders (e.g., law enforcement), on markets, and on consumer protection
ICANN, governments	Public policy research	Effect of ICANN policies. Example 1: gTLD Marketplace Health Index Assessment. Example 2: New gTLD program: follow-up and Subsequent Procedures PDP.	ICANN mission. ICANN contractual enforcement. Cybercrime research. Consumer protection.

Academic or Public Interest DNS Research	Tasks within the scope of this purpose include research studies about domain names published in the RDS, including information about the Registrant and designated contacts, the domain name's history and status, and domain names registered by a given Registrant (Reverse Query).

Template for defining an RDS Purpose:

Technical Issue Resolution -and- Academic or Public Interest DNS Research

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.

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.

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?

Working Group Notes 10 March 2018, ICANN61 F2F

DT1 Answers: Technical Issue Resolution

WG Response:

- Registrars do not want to be the first point of contact for Tech Issue Resolution – go to the hosting provider (or the Registrant/contact) first. All the Registrar can do is take the DN down. The web host is in a much better position to disable access to the hostname (not the DN)
- There are registrars whose business model includes serving as Tech Contact (value add)
- Is the entity you want to reach for tech issue resolution sometimes or always the account holder? Probably not since several different entities are enumerated in the DT's answer, but this deserves further discussion
- DNS OARC meeting example – DNSSEC validation – need to contact operators of the DN, to help resolve issue, not take the entire DN down
- What is the role of the Reseller in this purpose?
- It is not necessary that Registrants understand the technical issue – the "mechanics of the Internet" need to understand/resolve the issue being reported
- You only need the help of a domain contact when the IP isn't resolving
- Nameservers will not always lead to the hosting provider
- Hosting is not regulated by ICANN – that other part of the Internet community cannot be addressed by RDS policy
- Contacting the domain holder can also be useful if the site is partially pirated, to warn the owner. no need for the host to shut down the site, but for the domain holder to clean its database

DNS Research

- DT1 Answers: Academic or Public Interest DNS Research

WG Response:

- Note that #2, benefit to prospective buyer doesn't belong in this purpose – it's another purpose
- What is "public interest" research? Too open ended
- Universities typically apply a rigid protocol to research involving humans
- Do you need data associated with individuals for this purpose? Can't you just use aggregate data? Depends on the study – for example WHOIS Misuse study, WHOIS Accuracy study both used individual registrant and contact data to study misuses and inaccuracies to inform policy development, to the benefit of future registrants

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

Purpose Name: **Domain Name Management**

Definition: Collecting the required information to create a new domain name registration and ensuring that the domain registration records are under the control of the authorized party and that no unauthorized changes, transfers are made in the record.

Tasks:

1. Create registrant id; create domain name; add DNS data for domain name
2. Monitor domain name registration record for changes & correlate with activities
3. Manage set of domain names to keep them under the same administrative control
4. Transfer of domain name registration from one registrar to another or from registrant to new registrant.
5. Check registration database for status/existence of name when DNS does not work
6. Check contact information for ICANN policy compliance

Users:

These include:

- Registrant, gaining and losing registrar, registry, ISP & other operational contacts
- Domain name operational contacts, potential other users, UDRP, URS, WIPO, ICANN, court proceedings and enforcement actions
- Reseller and registrant affiliates
- New or gaining registrant
- Anyone attempting to interact with domain name for legal actions
- ICANN staff
- Local law enforcement , GAC public safety working group

Data:

Data Element	**Purpose**
Domain Name	Confirm domain name is registered.
Registrant Name	Identify registrant and determine if registrant is an organization or natural person
Registrant Organization	Identify registrant and determine if registrant is an organization or natural person
Registrant Postal Address (street address, city, state/province, postal code, country)	Monitor for any unauthorized changes to this data
Registrant Phone	One means of contacting the registrant for operational issues

Registrant Email	Contact the registrant for operational issues or verification of requests made to registrar to transfer or modify the domain name registration.
Registrar Name	Identify the domain name registrar to contact if registrant is not contactable
Registrar Abuse Contact	See above.
Original Registration Date	Ensure that the record associated with the domain name is maintained correctly
Creation Date	Ensure that the record associated with the domain name is maintained correctly
Updated Date	Monitor for changes to the registration data
Registrar Expiration Date	Monitor to ensure the domain name is renewed
Name Servers	Monitor to ensure the Nameservers have not been modified without authorization.
Technical Contact Name / Organization / Email / Phone	Contact with any operational issues
Administrative Contact Name / Organization / Email / Phone	Contact with any operational issues. Monitor for possible modifications in domain name management.
Registry and Registrar domain status	Monitor to ensure that the correct statuses are maintained for a domain name registration

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.

Tasks:

Real world user contacts the domain name registrant for information about their website or services offered using the domain name

Consumer protection – Internet user may reach out to an ISP to determine if the website is legitimate or if a suspect email is phishing.

Users:

These include:

- Anyone operating infrastructure on the Internet
- Any internet user that interacts with a website, service or is contacted via email from a domain name registration.

Data:

Data Element	**Purpose**
Domain Name	Confirm domain name is registered.
Registrant Name	Identify registrant and determine if registrant is an organization or natural person
Registrant Organization	Identify registrant and determine if registrant is an organization or natural person
Registrant Phone	One means of contacting the registrant for operational issues
Registrant Email	Contact the registrant for operational issues or verification of requests made to registrar to transfer or modify the domain name registration.
Registrar Name	Identify the domain name registrar to contact if registrant is not contactable
Registrar Abuse Contact	See above.
Creation Date	Newly registered domain names can be suspect for phishing
Updated Date	Monitor for changes to the registration data
Name Servers	Identify ISP for issues
Technical Contact Name / Organization / Email / Phone	Contact with any issues
Administrative Contact Name / Organization / Email / Phone	Contact with any issues

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. Inthe 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.

.

Working Group Notes 10 March 2018, ICANN61 F2F Individual Internet Use

DT2 Answers: Domain Name Management and Individual Internet Use

Domain Name Management

- DT2 Answers: Domain Name Management and Individual Internet Use

WG Response:

- Noted that WG Agreement 48 refers to legitimate purpose but does not give grounds for what criteria is used to determine legitimacy (e.g., consistency with mission)
- Legitimate interests of the parties should be identified – this is basis for lawful processing
- Third party legitimate interests are not limited to those of contracted parties.
- Benefit to the registrant is security and stability: To prevent unauthorized changes to the DN registration, that their DN doesn't get hijacked, that they have the ability to verify their DN's record
- The bylaws define, 4.6(e)(i) "Subject to applicable laws, ICANN shall use commercially reasonable efforts to enforce its policies relating to registration directory services and shall work with Supporting Organizations and Advisory Committees to explore structural changes to improve accuracy and access to generic top-level domain registration data, as well as consider safeguards for protecting such data."
- There are different ways of viewing security and stability, and from the registrant's perspective this purpose goes directly to security and stability

Individual Internet Use

Individual Internet Use

- DT2 Answers: Domain Name Management and Individual Internet Use

WG Response:

- Primary focus is identification and not contact
- Contact in the case of fraud may not be useful – contact might occur through other channels
- Would the average Internet user actually use WHOIS for this purpose?
- Should not be encouraging consumers to do this, but rather provide other consumer protection mechanisms
- Some users DO query WHOIS for this purpose – knowledgeable users are valid too
- WHOIS Review Team studied this very question. There is a study, including video footage, showing Internet users trying to find a domain name owner. The majority went to a website or search engine – WHOIS was not used. Since we paid for this study, we could use it. – RT4 – this question was part of this exercise. The majority went to the website or google. To say that WHOIS came up little if not at all. Perhaps we could retrieve this data for this purpose. For further information, please refer to the WHOIS Review Team's Final Report
- When you're engaged in a commercial transaction, you want tools to learn who you're dealing with, and why rob users of this tool? (imperfect or not)

Template for defining an RDS Purpose:

Domain Name Certification

Mailing list address: gnso-rds-pdp-3@icann.org
Mailing list archive: http://mm.icann.org/pipermail/gnso-rds-pdp-3/
Coordinated by: David Cake
Members: Kal Feher, Alex Deacon, Carlton Samuels, Jeremy Malcolm, Arsen Tungali

Template for defining an RDS Purpose:
Domain Name Certification

TEMPLATE:

Purpose Name: **Domain Name Certification**

Purpose:

Information collected by a certificate authority to enable contact between the registrant, or a technical or administrative representative of the registrant, to assist in verifying that the identity of the certificate applicant is the same as the entity that controls the domain name.

Definition:

The role of a certificate authority (CA) is to bind an identity to a cryptographic key in the form of a cryptographic certificate. In the case of TLS certificate issuance the CA also needs the ability the validate and verify that the identify of the certificate applicant is the same as the entity that owns the domain name (e.g. the Registrant). While the process and rigor of CA validation and verification procedures vary, both by the nature of the certificate desired and the processes of individual CAs, the WHOIS system can be used to validate the certificate applicants ownership of control of the corresponding domain.

Tasks:

A Certificate Authority may issue certificates with different validaton levels. The three levels of validation in standard use are Domain-validated, Organisation Validation, and Extended Validation. Domain-validated certificates require only demonstration of administrative control over the domain, and so do not require interaction with the RDS, and may be validated only using the DNS (optionally including other mechanisms such as email). They are therefore of limited relevance to this purpose.

Organisation Validated certificates require identification of the organization that requests the certificate, validation methods and levels vary. We have noted Extended Validation certificates as the most explicitly relevant to the purpose, but Organisation Validated certificates are also relevant. Guidelines for the Issuance and Validation of Extended Validation certificates may be found at https://cabforum.org/wp-content/uploads/EV-V1_6_5.pdf

Extended Validation certificates explicitly identify the legal entity that controls a web site as their primary purpose. They apply only to organisations, but for Business Entitys (as defined in the EV guidelines 8.5.4) the validation process requires confirming the identity and authority of individuals applying for certificates.

At a high level Certificate Authorities may perform the following tasks.

- Confirm that the enrolling organization (requesting the certificate) is listed as the Registrant in the WHOIS

- Send one of the WHOIS contacts (registrant/admin/technical) an email to confirm domain authorization/control
- Call one of the WHOIS contacts (registrant/admin/technical) to confirm domain authorization/control

Details of how this happens are defined in the CA Browser Forum's (CABForum) Practices Section 3.2.2.4 (https://cabforum.org/wp-content/uploads/CA-Browser-Forum-BR-1.5.2.pdf)

Section 3.2.2.4 of the Baseline requirements is explicitly required for Extended Validation certificates by rules 11.7.1 of the Extended Validation Guidelines.

3.2.2.4. Validation of Domain Authorization or Control

This section defines the permitted processes and procedures for validating the Applicant's ownership or control of the domain.

The CA SHALL confirm that prior to issuance, the CA or a Delegated Third Party has validated each Fully- Qualified Domain Name (FQDN) listed in the Certificate using at least one of the methods listed below .

Completed validations of Applicant authority may be valid for the issuance of multiple Certificates over time. In all cases, the validation must have been initiated within the time period specified in the relevant requirement (such as Section 4.2.1 of this document) prior to Certificate issuance. For purposes of domain validation, the term Applicant includes the Applicant's Parent Company, Subsidiary Company, or Affiliate.

CAs SHALL maintain a record of which domain validation method, including relevant BR version number, they used to validate every domain.

Note: FQDNs may be listed in Subscriber Certificates using dNS Names in the subjectAltName extension or in Subordinate CA Certificates via dNSNames in permitted Subtrees within the Name Constraints extension.

3.2.2.4.1 Validating the Applicant as a Domain Contact

Confirming the Applicant's control over the FQDN by validating the Applicant is the Domain Contact directly with the Domain Name Registrar. This method may only be used if:

1. The CA authenticates the Applicant's identity under BR Section 3.2.2.1 and the authority of the Applicant Representative under BR Section 3.2.5, OR

2. The CA authenticates the Applicant's identity under EV Guidelines Section 11.2 and the agency of the Certificate Approver under EV Guidelines Section 11.8; OR

3. The CA is also the Domain Name Registrar, or an Affiliate of the Registrar, of the Base Domain Name.

Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

Template for defining an RDS Purpose:
Domain Name Certification

3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact

Confirming the Applicant's control over the FQDN by sending a Random Value via email, fax, SMS, or postal mail and then receiving a confirming response utilizing the Random Value. The Random Value MUST be sent to an email address, fax/SMS number, or postal mail address identified as a Domain Contact.

Each email, fax, SMS, or postal mail MAY confirm control of multiple Authorization Domain Names.

The CA or Delegated Third Party MAY send the email, fax, SMS, or postal mail identified under this section to more than one recipient provided that every recipient is identified by the Domain Name Registrar as representing the Domain Name Registrant for every FQDN being verified using the email, fax, SMS, or postal mail.

The Random Value SHALL be unique in each email, fax, SMS, or postal mail.

The CA or Delegated Third Party MAY resend the email, fax, SMS, or postal mail in its entirety, including re- use of the Random Value, provided that the communication's entire contents and recipient(s) remain unchanged.

The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation. The CPS MAY specify a shorter validity period for Random Values, in which case the CA MUST follow its CPS.

Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.3 Phone Contact with Domain Contact

Confirming the Applicant's control over the FQDN by calling the Domain Name Registrant's phone number and obtaining a response confirming the Applicant's request for validation of the FQDN. The CA or Delegated Third Party MUST place the call to a phone number identified by the Domain Name Registrar as the Domain Contact.

Each phone call SHALL be made to a single number and MAY confirm control of multiple FQDNs, provided that the phone number is identified by the Domain Registrar as a valid contact method for every Base Domain Name being verified using the phone call.

Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.4 Constructed Email to Domain Contact

Confirm the Applicant's control over the FQDN by (i) sending an email to one or more addresses created by using 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' as the local part, followed by the at- sign ("@"), followed by an Authorization Domain Name, (ii) including a Random Value in the email, and (iii) receiving a confirming response utilizing the Random Value.

Each email MAY confirm control of multiple FQDNs, provided the Authorization Domain Name used in the email is an Authorization Domain Name for each FQDN being confirmed

Template for defining an RDS Purpose:
Domain Name Certification

The Random Value SHALL be unique in each email.

The email MAY be re-sent in its entirety, including the re-use of the Random Value, provided that its entire contents and recipient SHALL remain unchanged.

The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation. The CPS MAY specify a shorter validity period for Random Values.

Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

Note:

This group did not find that access to all RDS data was required in all cases, but was required for some CA validation methods.

Users: Describe the parties who often access gTLD registration data in pursuit of this purpose.

Employees of Certificate Authorities and automated systems associated with Certificate Authorities responsible for preforming the validation and verification as described above.

Data: List of gTLD registration data often involved in this purpose – for contact data, please identify the data subject (e.g., registrant, tech contact, registrar, etc.) and data element(s) as applicable.

Data Element	**Purpose**
Domain Name	To match with FQDN placed into the certificate.
Registrant, Tech and Admin *Email*	A means to contact the owner of the domain name, using manual or automated processes, with the goal of confirming that the identity of the certificate applicant is the same as entity that owns the domain name.
Registrant, Tech and Admin *Phone*	Used as an alternative method of contact in curcumstances where Email is not available or when an additional level of manual or automated verification is needed.
Registrant, Tech and Admin *Name*	Used when necessary to confirm an individual can or does work for or represent the applying organization.
Registrant, Tech and Admin Postal *Address (Street, City, State/Province, Country)*	Used to confirm that the organization of the entity that owns the domain name matches the organization of the of the certificate applicant. Also used in authentication/verification scenarios that are postal mail based.

Drafting Team 3 Domain Name Certification - Answers to Questions

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

A person who is able to demonstrate ownership or control over the domain name.

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

By ensuring the certificate is granted only to an entity that is able to demonstrate ownership or control over the domain name, the trustworthiness of the certificate system is increased, in order to better achieve the primary goal, which is to enable efficient and secure electronic communication.

Reference: CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates version 1.5.6, (henceforth the CA/B Baseline Requirements)

section 1.4.1 Appropriate Certificate Uses

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

An applicant for a Certificate must prove their control or ownership of the domain name before a certificate can be granted by a CA, which 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, as set out in section 3,2,2.4 of the CA/B Baseline Requirements

There are three methods that use the RDS.

Method 3.2,2.4.1 is to use the RDS to confirm the applicant is the domain contact. This method may only be used if the personal identity of the domain contact has also been confirmed by methods outside the RDS (eg the methods in section 3.2.2.1 of the CA/B Baseline Requirements, or the Extended Validation equivalents, or the CA is also the registrar (see also 3.2.2..4.12)). It is to be expected that the domain contact will have consented to, and practically facilitated, the confirmation of their personal identity by means outside the RDS, if they wish to use this method, and also the CA must be able to access the domain contact data. A person identified by this means must also remain a current domain contact in order to make any certificate changes. This method requires ongoing access to domain contact personal identifying information. There may be cases where access to additional personal identifying information beyond Domain Contact name is required for disambiguation purposes, as names are not unique identifiers.

Method 3.2.2.4.2 is to use Email, Fax, SMS, or Postal Mail
This method requires the applicant to provide one of these forms of communication to the CA that is visible within the RDS and ascribed to a domain contact, accessible to the CA to use, and that the domain contact can access. It is not necessary that the applicant uses those means to reply to the CA, only that they are able to supply a Random Value communicated to them.

Method 3.2.2.4.3 is via phone.
This method requires the applicant to provide a phone number associated with the Domain Contact within the RDS, and to make that information accessible to the CA. This requires both phone information and domain contact information. This method is only effective if the information is valid and may be used to initiate a phone conversation with the domain contact.

There are multiple other methods for verifying control, that we have not described in detail, as they do not use the RDS. There are a range of technical methods that rely on demonstrating control and access to either services that are run directly under that domain name (for example, mail service 3.2.2.4.4, web sites 3.2.2.4.6, TLS 3.2.2.4.9 and 3.2.2.4.10), or the DNS itself (3.2.2..4.7).

It is worth noting that the only non-technical method of verification that does NOT also require information from the RDS, method 3.2.2.4.5, Domain Authorisation Document, will no longer be valid for use after August 2018. We recommend this method is ignored for purpose of working group deliberation at this point for that reason.

In addition to the above, we should also note the requirements for more advanced forms of certificate, the Organisational and Extended Validation Certificate, The drafting team wishes to separate discussion of these form of certificate, as this discussion is primarily to demonstrate their inapplicability for purposes of this question within this working groups scope.

Discussion of Extended Validation Certificates

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

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 identified and validated by independent means to the RDS.
Reference. CA/Browser Forum Guidelines For The Issuance And Management Of Extended Validation Certificates version 1.6.5, section 11.8 and 11.9

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

The purpose of an Extended Validation certificate is to identify the legal identity that controls a web site, and to enable Encrypted Communications.
Reference. CA/Browser Forum Guidelines For The Issuance And Management Of Extended Validation Certificates version 1.6.5, section 2.1 and 2.1.1
Secondary purposes include establishing business legitimacy and mitigating various forms of online identity fraud (section 2.1.2), but not establishing business honesty or trustworthiness (2.1.3)

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

With regard to the applicant, it is expected that they are verified as a registered holder, or controller, of the Domain Name(s) to be included in the EV Certificate; (11.1.1. (2)).

This must be performed via one of the methods in the CA/B Baseline Requirements section 3.2.2.4. and additional checks must be performed on domain names that utilise multiple character sets.
Reference CA/Browser Forum Guidelines For The Issuance And Management Of Extended Validation Certificates version 1.6.5, section 11.7
There are additional requirements for certificates issues to .onion names, but these are not part of the Domain Name System and not relevant to this working groups scope.
There are many additional requirements for Extended Validation Certificate, but that do not vary dependent on the Domain Name, and do not utilise the RDS (and are generally required to be verified by means wholly independent of the RDS), and so are outside the scope of this working group.

So discussion of the requirements of 3.2.2.4 of the CA/B Baseline Requirements is relevant to Extended Validation Certificates, but the other requirements of Extended Validation certificates are outside the scope of this working group.

Working Group Notes 10 March 2018, ICANN61 F2F

Domain Name Certification

- DT3 Answers: DT3AnswerstoQuestions-8March.pdf

WG Response:

- Who is the certifying agent? The CA itself
- This purpose is only relevant to those registrants that want a certificate; access could be provided by some kind of one-time-use token and not publication of data
- When DN is sold, is the certificate revoked?
- ICP in China and SSL: having public email makes it much easier. We face difficulties with .co.uk to get SSL validation, because email is not available in WHOIS by design
- In cases where email address is published in WHOIS, obtaining a certificate may be easier, but email-based validation is not the only method available and not having an email address doesn't prevent obtaining a certificate
- If a CA (other than the CA run by the registrar) wants access to data to provide their service they could pay the registrar to get access. These kinds of business model issues are out of scope of this PDP.

Purpose Name: **Domain Name Purchase/Sale**

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.

Tasks: Parties purchasing or selling a domain name often engage in the following tasks.

1. When making purchase queries about a domain name, registration data is used to determine the current Registrant and how to contact them.
2. When making purchase queries about a domain name registered using a Privacy or Proxy service, registration data allows a potential buyer to determine how to contact the current domain name user/owner by relaying communication through the Privacy/Proxy service provider or through a legal contact.
3. During acquisition, purchasers not only need to find out who they should contact, but also the history of the domain name's registration to confirm prior associations and to ensure that there are no issues with buying a domain name "fit for purpose."
    - WHOIS history also provides information about merchantability. For example, when buying a house, buyers do a title search to certify ownership and ownership custody chain. Similarly, domain name buyers commonly search WHOIS records before and after sale to verify the old and new Registrant are accurately recorded.
    - Additionally, some domain name buyers consider the WHOIS history as significant for understanding a domain name's reputation via prior registrant WHOIS data. For example, brokers may update WHOIS data before offering domain names for sale; in such cases, assessing the domain name's reputation requires looking beyond current WHOIS data to identify past registrants, as well as historical information about the domain name obtained from other sources.
4. Registration data is also used during due diligence research to identify the current Registrant of the domain name, confirm whether they have a relationship with the Registrant Organization, and to determine other domain names with which buyers or sellers may be associated.

5. In summary, registration data: informs buyers and sellers and those they are working with; facilitates verification that parties can sell/buy the domain name; makes it possible to carry out the purchase/sale transaction; and can assist with verification (with a third-party) that the domain name has actually changed hands before final payment is made from escrow.

Users: The following parties often access gTLD registration data in pursuit of this purpose:

User Role	Description of RDS User's Role in Domain Name Purchase/Sale
Third-party Buyer	Any individual or entity (e.g., small business owner, corporation, domain name broker) that is attempting to buy a domain name from a registrant.
Domain Broker	A broker who may be purchasing, facilitating a purchase or sale, or facilitating the exchange of monies for a purchase a sale on behalf of a registrant or third party purchaser.
Registrant	Person or entity that currently holds the rights to a domain name being purchased.

Data: The following gTLD registration data is often involved in this purpose.

Data	Description of Registration Data used during Domain Name Purchase/Sale
Registrant Name	Current registrant of the domain name so interested buyers or businesses know *who* to contact for purchase.
Registrant Contact	A way to contact the current registrant, via email or phone, to make an offer for domain name purchases or for legal purposes, e.g., notifications of trademark infringement.
Registrant's Country	In purchasing a domain, country of origin provides jurisdictional context for local laws and procedures throughout the transaction.
Date of Registration	To establish historical ownership of a domain name to assess the name's merchantability**.**
Domain Names for Specified Registrant	EWG recommendation for new search capability to facilitate transfer of all domain names owned by a single registrant or company in the case of a merger/transition.

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.

Working Group Notes 10 March 2018, ICANN61 F2F

Domain Name Purchase/Sale

- DT4 Answers: Domain Name Purchase/Sale

WG Response:

- The expectation is that a potential buyer can verify the seller owns the DN; this is not a requirement for public access – for example, a DN registrant could supply a lookup key to the buyer
- At what point would this be opened up to verification – after initial inquiry, or when the seller chooses to go forward?
- Potential buyers may want to see a registrant's full portfolio, not just one DN
- Is this purpose limited to business-owned DNs or does it apply to all DNs?
- Should it be a requirement to be able to find out the full set of domains controlled by a single entity, or is this just a particular desire?
- A potential buyer should send a note to the account holder, via the registrar
- Why is there a need for the account holder to have control of a DN?
- The account holder is not always the registrant and may not have the ability to sell a domain name
- Ultimately it should be the potential seller that controls further communication for this purpose
- Are there two different audiences? All registrants, or only those that express interest in being contacted for this purpose?
- There may be value in supplying additional information, but it seems this may be best handled outside of the basic system, e.g. by exchanges for listing names potentially available for sale
- Is there any threshold for the buyer is identifying itself as a bona fide purchaser?
- Are there two different types of entities being contacted in the beginning of this purpose? (1) any registrant that may or may not be interested in selling names; (2) registrants that specifically wish to receive potential purchase offers for their DN?
- To what extent must this be supported by the mandatory system as opposed to external services that have developed and will continue to develop?
- The buyer needs to have a third-party place to verify the registrant holds the rights to the DN – a public record of ownership, not just the current contact information
- If the seller opts in to full disclosure of other DNs, that could be done at the seller's discretion, based on an incentive (e.g., paying more for the DN)
- There's a sharp distinction between validating whether the seller has title versus whether the car is in running order. For the latter, the state does not participate; the buyer would get an assessment from their own mechanic
- Being contactable for this purpose is different from publishing contact data for this purpose
- The info listed in the Registrant field is supplied by the Account Holder, and it's entirely possible that the information is unrelated to the account and domain.

RDS PDP WG DT5 Deliverable 8 Nov 17

Purpose Name: **Regulatory**

Definition:

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

Tasks:

- Regulatory authority to ensure that registrants, registries and/or registrars are compliant with applicable laws such as data protection, user privacy, tax law, etc.

Users:

- Tax collection agencies may request access registration data to identify identification of contacts for domain name used for on-line sales.
- Regulatory agencies may want to access registration information for many purposes: law enforcement investigations, legal compliance, , etc.

Data:

- Data tending to establish the identity and/or location of domain name registrant. For example, Registrant Name and Registrant Address (at least province/country address).
- Data that tend to categorize the type of users: individual, corporation, organization, academic, etc. The types of users may result in different tax systems or different compliance standards.

Specific data elements by use case:

1. Investigation into fraudulent and inaccurate information (by government and/or regulatory authority):
    - Registry Expiry Date
    - Registrant Name
    - Registrant Email
    - Name Server
    - Registrant Name
    - Registrant Phone

- Log files and, … other records associated with the Registration containing dates, times, and time zones of communications and sessions, including initial registration
- Name server status

2. A tax authority may require the following data elements for billing and tax collection purpose
   - Domain Status
   - Domain Name
   - Registrant Name
   - Registrant Street
   - Registrant Email
3. A government agency
   - Domain name
   - Registrar Whois Server
   - Registrar URL
   - Update date
   - Registry Expiry Date
   - IP address
   - Registrar
   - Registrar abuse contact email
   - Reseller
   - Domain status
   - Registrant Name
   - Registrant E-mail
   - Admin name
   - Tech ID
   - Name server
   - Billing Contact name
   - DNSSEC
   - Registrar WHOIS server

RDS PDP WG DT5 Deliverable Redline Draft 8 November 2017

Purpose Name: **ICANN Contractual Enforcement**

Definition:

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

Tasks:

- Monitoring and investigation by ICANN Compliance of performance of contract terms.

Users:

- ICANN Compliance audit and respond to complaints about non-compliance by contracted parties (e.g., data inaccuracy or unavailability, UDRP decision implementation, transfer complaints, data escrow and retention).

Data:

ICANN organization may require the following data elements to check ICANN contractual compliance

- Registrant Name
- Registrant Street
- Registrant Email
- Registrant Email
- Name Server
- Domain Status
- Log files and, … other records associated with the Registration containing dates, times, and time zones of communications and sessions, including initial registration
- Updated Date
- Registry Expiry Date

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
     - 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.

March 2018

RDS Purpose: ICANN Contractual Enforcement
Emails to maguy.serad@icann.org from Chuck Gomez on behalf of GNSO RDS-PDP-5
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.

Correct - ICANN Contractual Compliance, as part of its compliance process (https://www.icann.org/resources/pages/approach-processes-2012-02-25-en), identifies the registrar and/or registry operator of the domain name and undertakes various activities to ensure compliance with contractual obligations.
Compliance does not currently reach out to the domain name's registrant unless the registrant is also the person submitting the complaint ("reporter"). Compliance may check the WHOIS data to confirm whether the reporter of the complaint is the current registrant of the domain name. Compliance may also follow up with the reporter to validate the complaint before collaborating with the registrar or registry operator on the complaint. Compliance may also receive communications between the registrar or registry operator and the registrant during the course of processing the complaint. For example, a registrar may provide evidence of emails with the registrant during a WHOIS inaccuracy investigation or transfer complaint investigation.

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.
- Commented

Correct - The objective of ICANN Contractual Compliance in contacting registrars, registry operators and complaint reporters (who may also be registrants) is to fulfill the compliance function of enforcing ICANN agreements and policies.

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.

Correct -ICANN contracted parties and complaint reporters (who may also be registrants) are expected to demonstrate compliance (contracted parties) and/or facilitate ICANN's determination of whether the complaint is in scope of the relevant ICANN agreements and policies (reporters).

DT5 ICANN Contractual Enforcement – Slide 9

- DT5 answers introduced by Beth
- WG was joined by ICANN compliance staff Selim Manzak, Jennifer Scott, and Maguy Serad
- Compliance staff confirmed that:
    - ICANN does NOT use registrant data to initiate contact with registrants – as ICANN does not have contractual relationship with registrants, ICANN notifies the contracted party instead (e.g., Registrar)
    - ICANN DOES use registrant data to investigate complaints and enforce compliance with contractual obligations – for example, to investigate unauthorized use of another's name or address in a registration
    - Compliance cannot at this point make any assumptions about how the GDPR compliance model will impact their procedures or use of registration data

RDS PDP WG – Drafting Team 6: Legal Actions

Purpose Name: **Legal Actions**

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.

Tasks:

1. Identify registrant contact information associated with a domain of interest for potential legal action
2. Use of reverse query to identify and combat use of fraudulent contact data in a domain registration
3. Access and review historical domain name registration associated with a domain of interest for potential legal action
4. Use of reverse query to identify all domains registered with a given name or address associated with a domain of interest for potential legal action
5. Identify registrar, registry and IP address/es associated with the domain of interest

Users:

These include:

- Individuals or entities (or their representatives) who have been victim of harm / wrongdoing associated with the domain of interest
- Individuals or entities (or their representatives or service providers) who are concerned that their name, address or other contact information has or will be used fraudulently by a third party to register a domain or obtain other services
- Intellectual property owners (or their representatives or service providers) in order to investigate and enforce their rights where infringing activity is associated with the domain of interest
- Operational security, anti-abuse, merchant monitoring service or domain reputational professionals (or their representatives or agents) in order to investigate and respond to potential abuse including escalating same to possible civil or criminal enforcement
- Non-LEA governmental agencies to investigate and enforce civil violations of law associated with the domain of interest
- LEA, prosecutors, or other governmental actors to investigate and enforce against possible criminal activity associated with the domain of interest or its registrant. This has been used, for example, to investigate cybercrimes, money laundering, and sexual exploitation of children. There is also anecdotal evidence of LEA in certain countries using registrant data to investigate and/or prosecute possible crimes committed by journalists or protesters who have registered the domain of interest, such as blasphemy.

- A person or entity (or their representatives) in order defend a claim related to one of the aforementioned types of legal action for purposes of due process, to provide exculpatory evidence, etc.
- Legal counsel, their clients, and their respective authorized agents.

Data:

These include the following, both for use of the individual data item and to aid in determining attribution and correlation to other relevant data as necessary to support the purpose

Data Element	**Purpose**
Domain Name	Confirm domain name is registered.
Registrant Name	Ascertain registrant identity, including to help determine the relationship between the registrant and the potential legal action.
Registrant Organization	Ascertain if registrant is a legal person, or is an individual registrant affiliated with an organization or legal entity.
Registrant Postal Address (street address, city, state/province, postal code, country)	Ascertain registrant location both for jurisdictional analyses as well as identifying relevant government or law enforcement agencies for criminal referral, as applicable. Used for service of legal process and providing correspondence and legal notices in hard copy by mail.
Registrant Phone	A means of contacting registrant beyond email or postal mail, if necessary, particularly for urgent requests.
Registrant Email	A means of contacting registrant in writing with legal action (where permitted in the relevant jurisdiction), or related inquiries or requests (cease and desist letters, informal notices of legal action, etc.).
Registrar Name	Identify the domain name registrar to determine jurisdiction of registration authority for various legal purposes (in rem actions against domain name, secondary liability, third party subpoenas, court orders obligating the registration authority to take action, etc.), or to contact registrar in connection with a takedown, hold, or lock request or other inquiry concerning the domain name.
Registrar Abuse Contact	See above.
Original Registration Date	The date on which this domain name was first registered. Generally helpful to establish rough timelines concerning the alleged harm / wrongdoing / illegal activity at issue, such as in a trademark enforcement context to determine if registration predated establishment of trademark rights. .
Creation Date	The latest time that the domain name was registered; it is possible that the domain name was previously registered and subsequently deleted multiple times. See above regarding Original Registration Date – helps establish timeline for purposes of enforcement or investigation into various forms of harm / wrongdoing / illegal activity.
Updated Date	Helps establish timeline for purposes of IP enforcement or anti-abuse investigation, including most recent renewal date or to signal other recent changes to registration data or domain status.
Registrar Expiration Date	Identify possible expiration or renewal date of the domain name, which may signal when the infringing, abusive or other illegal activity may cease (if

	domain is not renewed) or might become available for defensive registration and avoid need for further legal action.
Name Servers	Identify whether domain name is associated with any content, and if so, identify the specific IP address(es) and hosting provider(s) in order to contact hosting provider with takedown requests or other inquiries relating to the domain/website helpful to enforcement one's rights, mitigate the harm, and/or further investigate the alleged harm / wrongdoing / illegal activity.
Technical Contact Name / Organization / Email / Phone	Identify technical contact for anti-abuse response or to investigate or address the forms of harm / wrongdoing / illegal activity that are technical in nature
Administrative Contact Name / Organization / Email / Phone	Identify administrative contact for anti-abuse response or other inquiries where there is no response from registrant (assuming there is a separate admin contact).

ANNEX A

The legal actions purpose generally includes the following tasks:*

Task	Description
1. Identify registrant contact information associated with a domain of interest for potential legal action	Identify name, address, location, email address, phone, etc. of domain registrant to • help identify the potential defendant / alleged wrong doer; • be able to contact registrant and for follow through; • determine the jurisdiction for possible civil litigation or criminal referral; • prepare for, and initiate a civil litigation, arbitration, UDRP/URS action, or similar non-criminal process; • prepare for, and initiate a criminal litigation or similar criminal process. Such wrong doing / illegality may include consumer fraud or deception, unfair competition, passing off, intellectual property infringement, computer fraud and abuse, or similar activity where there is the possibility of a civil or criminal remedy to address the alleged wrongdoing. It may include civil action by private actors (such as consumer fraud claims or IP infringement claims), civil enforcement by governmental authorities (such as consumer deception, unfair competition, tax evasion, etc.), and criminal enforcement by LEA, prosecutors, or other governmental criminal enforcement agencies. In certain cases, such action might include pursuing individuals or organizations to suppress or prosecute acts of free speech, political activity, or acts deemed to be blasphemous under the laws of certain countries. It may also include other related uses such as UDRP/URS providers to confirm registrant details in a filed action, ICANN for contractual compliance purposes, and operational security professionals or domain reputational professionals who may escalate matters for civil or criminal enforcement. Such information is relevant for domain name arbitration or other legal proceedings; for purposes of due process and establishing jurisdiction, and contacting the registrant or their legal representative, prior to taking legal action and then taking legal action if the concern is not satisfactorily addressed.

Task	Description
2. Use of reverse query to identify and combat use of fraudulent contact data in a domain registration	Identify and respond to fraudulent use of legitimate data for domain name registration by using a Reverse Query on identify-validated data. For example, this could include a legitimate registrant using such a query to identify if there are domains that are either registered to him/her/it that the registrant did not register, or that use the legitimate registrants address or other points of contact without authorization. This could also include investigation into the fraudulent use of a person/entity's contact information by another for a domain registration.
3. Access and review historical domain name registration associated with a domain of interest for potential legal action	Enable historical research about a domain name registration (whowas) to help identify persons/entities/locations that have historically been involved with a domain that is the subject of potential legal action
4. Use of reverse query to identify all domains registered with a given name or address associated with a domain of interest for potential legal action	Enable research into the potential defendant / alleged wrong doer to determine if the alleged harm / wrong doing / illegality extends to other domains registered to the name or address.
5. Identify registrar, registry and IP address/es associated with the domain of interest	Determine location/jurisdiction of domain name registration authorities and IP addresses/servers associated with the domain for purposes of *in rem* proceedings involving the domain alleged to engage in harm / wrongdoing / illegality and/or requests for third party subpoenas in connection with a civil action against the domain of interest or its operator.

** In each case, it is also possible to perform the task to refute a claim against a defendant in a legal action.*

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.

Working Group Notes 14 March 2018, ICANN61 F2F

DT6 Legal Actions – Slide 10

- DT6 answers introduced by Griffin –
- Focus is on contracts between private parties (i.e., not contracts with ICANN)
- Possible to accomplish 2d) using IP addresses associated with domain names or Nameservers
    - DT6 had agreed to replace "hosting provider" by "DNS operator" throughout answers
    - Nameserver does not always lead to responsible party – investigative value
    - Why does DT6 (3) refer to "Legal Authority" is communication is between private entities?
        - Answers cover both cases where private entities initiate communication (e.g., a private corporation pursuing a legal action), and also cases where legal authorities have gotten involved in investigating allegations
        - Contacted entity may be more likely to respond to a legal authority than private party – see last bullet under question 3
        - Contacted entity may be under no obligation to respond
        - Some feel that "Legal Action" is too broadly defined

Template for defining an RDS Purpose:
Criminal Investigation or DNS Abuse Mitigation

Overall Purpose Name: **Criminal Investigation or DNS Abuse Mitigation**

Definition: The broad category of criminal investigation 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.

Overall Purposes:

Criminal Activity/DNS Abuse - Investigation

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..

Criminal Activity/DNS Abuse - Notification

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..

Criminal Activity/DNS Abuse – Reputation

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..

Users[1]: The primary actors in these scenarios include law enforcement, regulatory authorities, cybersecurity professionals, IT administrators, and automated protection systems. Additional

[1] The DT recognizes that the list of users may ultimately need to be narrowly defined to allow for authorized / authenticated access to agreed upon data elements. This applies to all instances in this document where users are mentioned.

actors may include nearly anyone attempting to either track down the source of an online abuse they have experienced or attempting to determine the authenticity of a website or e-mail communication.

Tasks: Using information from the RDS, these actors will, depending upon the circumstances: contact domain owners and/or the entities that provide services for an affected domain to mitigate problems, gather evidence, or notify them of compromises; expand investigations and associations to fully understand the scope of an abuse issue; identify Internet infrastructure involved with detrimental activities, inform protection systems to take protective actions; and, if appropriate and justified, request suspension of domain names.

Data Elements used generally for criminal investigation or DNS Abuse Mitigation

Domain WHOIS record

- Registrant (Name, Address, email address). Use - identification, information and intelligence gathering etc
- Creation date, renewal date, last updated date, expiry date. Use - is it recently registered (maybe a DGA etc) ; Is it a long time registered / historic domain - if so perform a WHOIS history check on it to look at identifying the registrant...before they changed over to a privacy/proxy registrar to hide their details
- Registrar. Use - further enquiries with an disclosure authority/court order.
- NS records (Nameserver - used to direct the traffic of your website to a specific web server at a web host.) Use - what other domains point to this NS - this could provide you with a whole host of intelligence on other domains controlled by the same person/organisation.

Network WHOIS record

Abuse contact (for further enquiries - disclosure authorities)

CIDR space of network provider (use - if they own for example a /24 - try some passive DNS to see what other domains point to these IPv4 addresses - may give you more intelligence on malicious domains associated to a rogue server etc)

DNS records

MX record. Use - which network provider provides mail for the domain ?

Bad WHOIS data of value

A false domain name, registrant, address, email

Template for defining an RDS Purpose:

Criminal Investigation or DNS Abuse Mitigation

Uses - bad/false/stolen/incomplete domain whois data may give an investigation a new lead in terms of intel gathering, linked accounts showing the same false data through a registrant search of the WHOIS record for similarly registered domains.

Template for defining an RDS Purpose:
Criminal Investigation or DNS Abuse Mitigation

Background: This category encompasses a broad set of use cases for querying different data elements associated with one or more domain names contained in the RDS. The data queried will depend upon the nature of the detrimental activity in question, the goals of the person or entity making the queries, and the stage of an investigation or incident at the time. For some tasks a deep set of data may be needed for a particular domain or small set of domains, while for others, a very small amount of data may be needed per domain, but for a very large number of domains. Given this wide variety of use cases, data access, and contact needs, this document will present several example use cases grouped into logical categories of purposes.

The broad categories of purposes we propose to use for logical grouping include investigation, notification, and for creation of reputation. These are quite broad and may not be sufficiently granular for use in legal language, but do provide useful groupings for the primary purposes that fit into these categories. Below are three proposed purposes to address these three broad categories.

Investigation:

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..

Notification:

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..

Reputation:

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..

Template for defining an RDS Purpose:
Criminal Investigation or DNS Abuse Mitigation

Within these three broad purposes there are several categories of usages and actors that may require further definition and the document provides some non-comprehensive examples of these categories of uses within the various purposes. The first category distinction is between individual investigators or small teams looking into discrete incidents making ad-hoc data requests for single or small sets of domains, and automated processes that may query for information about thousands to millions of domains in a very short time period.

A second axis of differentiation of use cases differentiates between the various stages of an investigation/mitigation/protection effort. First, the use of RDS data to determine the likely involvement of a domain name as one registered and controlled exclusively to perform the detrimental activity or one that has been compromised and used against the wishes of the domain registrant. Second, a set of use cases for using RDS data to understand the scale and scope of domains and Internet infrastructure being used in conjunction with a particular attack or campaign.

A separate category of uses of RDS data within the "investigation" category of use cases encompasses use in those cases where the domain name itself isn't necessarily the focus of the investigation or abuse concern. Domain names can be tangentially involved in other cases ranging from online abuses to real-world crimes. Access to information in the RDS may further such investigations when it is determined for example that a potential miscreant may have registered domain names for his or her personal use or a domain name may have been associated with evidentiary e-mails. In such cases, understanding who may have registered or been involved with supporting a domain may lead to further evidence leads.

Note:
This table is largely based on current practices and currently available data unless otherwise noted.
One capability discussed in this document that exists outside of the current whois system (with some exceptions) is the concept of "reverse whois". Such services exist and provide high value information to inform many use cases/purposes in this category. Some form of reverse whois has been proposed for a future RDS and/or the accommodation of such services within the RDS framework. This work explains how those services are used and useful today without commenting upon their appropriateness now or in the future.
Using new data elements like "social media contact" or other proposed future RDS capabilities is not explored here. Where such data elements were to be collected in the future, these use cases would need to be updated to reflect their applicable use. For example, a preferred contact method that is a unique identifier is a good candidate for pivoting on investigations to expand their scope, and of course, if a registrar prefers to receive an SMS message to report abuse, processes that involve registrar contacts would incorporate that data element.

Table of purposes and associated use cases

Section 1: Investigations

Subsection 1A: Determination of domain status (malicious/compromised)

Template for defining an RDS Purpose:
Criminal Investigation or DNS Abuse Mitigation

1A-1 Purpose Name: Manually determine if the domain of a website used for an attack is compromised or registered maliciously

USE CASE VERSION: Access information held on a domain name to enable security professionals and law enforcement to determine if the domain of a website used for an attack is compromised or registered maliciously.

Definition: Determine if domain of website used for an attack (e.g. phishing, exploit, scam, etc.) is compromised, being abused, or registered maliciously. Websites used for online abuse fall into one of three categories: compromised - hacked or exploited where unauthorized content is added to the site, abused - a hosting service is misused by a bad actor, or registered maliciously by the miscreant directly. Determining this status is critical for informing the next steps of an investigation or mitigation.
Tasks:
1) Obtain a potentially abusive domain name from a report of some sort - typically an abuse report.
2) Verify abusive activity is occurring
3) Query RDS data for information about the domain including age, registrar, registrant/admin/tech/abuse contacts
4) Use known techniques and infrastructure of both "good" and "bad" actors to determine likelihood of a malicious registration. Prime factors include age of domain, nameservers of domain, registrar of domain, reseller of domain, privacy service employed (particularly for phishing), known registrant (good/bad), other known contacts. Note that for a malicious domain, the data for registrant will be false, but if it matches other known "bogus" data, this is a positive attribution factor. One data element that will be constant between malicious registrations is the registrant e-mail address which provides control over a domain in many circumstances. A domain "handle" is also useful for such matches.
Users: Security researcher, LE researcher, automated tools used by researcher
Data: Creation date, nameservers, registrar, reseller, full available contact information for registrant and any other contacts (e-mail and contact handle most useful)
Subsection 1B: Contacting appropriate parties/taking action

1A-2 Purpose Name: Automatically determine if a domain used for an attack is registered maliciously

NEW VERSION: Access information held on a domain name to enable automated security systems to determine if the domain of a website used for an attack is registered maliciously.

Definition: Determine if domain used for an attack (e.g. phishing, exploit, spam, scam, etc.) is compromised, being abused, or registered maliciously. Domains used for online abuse fall into one of three categories: compromised - hacked or exploited where unauthorized content is added to the site, abused - some hosting service is misused by bad actor, or registered maliciously by the miscreant directly. Determining this status is critical for informing the next steps in preventing a risky connection.

Template for defining an RDS Purpose:
Criminal Investigation or DNS Abuse Mitigation

Notes: These activities are not well served by the current asynchronous and slow response that the current whois system provides. Thus while some networks incorporate such queries, most use pre-positioned reputation data aggregated by third-party specialists to make the described decisions.

Tasks:

1) Obtain a potentially abusive domain name from a live stream of data – e.g. e-mail server connection requests, outbound network requests at the DNS resolver, pre-fetching activities of browsers on a corporate network or requests to a WAF (Web Application Firewall).
2) Query RDS data for information about the domain including age, nameservers, and registrar. Other data such as contact data would be desirable, but response time is usually too slow to reliably use.
4) Use known techniques and infrastructure of both "good" and "bad" actors to determine likelihood of a malicious registration. Prime factors include age of domain, nameservers of domain, and registrar of domain.

Users: Automated security processes/systems including but not limited to e-mail servers, firewalls, DNS resolvers, and WAF's.

Data: Creation date, nameservers, registrar

Subsection 1B: Investigate domain ownership or operations for domain tied to real-world criminal/abuse activities

1B-1 Purpose Name: Determining domain ownership or involvement with operating a domain name tied to real-world criminal/abuse activities

NEW VERSION: Access information held on a domain name to enable security professionals and law enforcement to determine domain ownership or involvement with operating a domain name tied to real-world criminal/abuse activities.

Definition: Domain names can be tangentially involved in other cases ranging from online abuses to real-world crimes. Access to information in the RDS may further such investigations by providing ownership or operational connections to a domain name that has come up as evidence or a potential lead in a case focused on behavior not primarily tied to that domain. For example, e-mails may indicate that a miscreant used a domain name to commit fraud or some other act, or an e-mail address tied to a threat like a botnet was used to register one or more domain names.

1) Determine that a domain name is potentially indirectly involved with in a crime or incident via an investigation.
2) Access RDS data to obtain full registrant and potentially admin contact data.
3) Evaluate the information returned to determine if actual contact data is included, or if it is bogus or privacy protected to determine if the domain registration is providing actual data.
4) Use real data to significantly supplement tangential investigation. Add bogus or suspect data to investigatory file.
5) If applicable, pivot off data found in this use case to expand to other potentially related domains.

Template for defining an RDS Purpose:
Criminal Investigation or DNS Abuse Mitigation

Users: Law enforcement personnel, security researchers, CERT teams, first responders
Data: Full available contact information for registrant and any other contacts (e-mail, phone number, and contact handle most useful), nameservers, registrar, reseller, creation date
Subsection 1C: Scoping infrastructure involved in issue

1C-1 Purpose Name: Expand knowledge from one known malicious domain to other domains potentially part of the same issue

NEW VERSION: Access information held on a domain name to enable security professionals and law enforcement to expand knowledge from one known malicious domain to other domains potentially part of the same issue.

Definition: Investigate key attributes of a known malicious domain to find others that may be part of the same or related incidents. Since criminals/abusers often re-use common elements for registering malicious domains, once a domain has been identified as being malicious, researchers can take key unique elements from that domain and search for other domains sharing those elements. Such unique elements often include unique nameservers, unique contact data – particularly registrant and/or admin contact e-mail or to a lesser extent, phone number. This purpose requires the existence of some sort of "reverse whois" capability where an RDS, cached database, or third party collection of RDS data can be queried on an attribute and return a list of all domains sharing that attribute. Such domains tend to cluster on less unique elements such as creation date, registrar, and reseller, but using these data elements requires other meta data for correlation. Lists of suspect domains may then be probed to see if they exhibit the same illegal/abusive behavior.
Tasks:
1) Obtain a positively identified malicious domain from prior investigation, trusted data feed, or other high-confidence source.
2) Query RDS for key attributes that allow for "pivoting" to other potentially related domains. Such information will include nameservers, full contact data for registrant, admin, and in some cases tech contacts (particularly unique elements like contact handle, e-mail address and phone number), and other more loosely associable elements like registrar, reseller, and creation date.
3) Determine veracity of supplied information as an informative element. Accurate data is not necessary in this step since repeated bogus data is a strong indicator of associated abuse.
4) Build list of domains based on reverse whois lookups on unique elements.
5) Examine list of domains for the same abusive behavior or indicators that they may have been or will be used in a similar matter
6) Use the gathered data to again pivot on unique elements found within the newly discovered domains.
7) Use an investigatory tool like a relationship visualization system to "cluster" domains that have paths of relationships to look for patterns, key elements, and potential clues as to how the miscreant may create new domains in the future.
8) Use this information to inform other processes like mitigation or criminal investigations.
Users: Law enforcement personnel, security researchers, CERT teams, first responders

Template for defining an RDS Purpose:
Criminal Investigation or DNS Abuse Mitigation

Data: Full available contact information for registrant and any other contacts (e-mail, phone number, and contact handle most useful), nameservers, registrar, reseller, creation date

1C-2 Purpose Name: Examine all domains sharing one or more key elements tied to abuse to determine if a larger issue exists

NEW VERSION: Access information held on a domain name to enable security professionals and law enforcement to examine all domains sharing one or more key elements tied to abuse to determine if a larger issue exists.

Definition: Individual data elements that appear in RDS data are often identified in investigations as being associated with abuse. For example, these could include a phone number used by a serial scammer, an e-mail address used in prior security incidents or malicious registrations, a PO box of a known criminal operation. Using such elements and reverse whois queries, an investigator can find domain names likely to be associated with malicious activities and examine them for abusive behavior and/or monitor them for future activities.

1) Obtain a positively identified malicious or suspicious data point that represents a unique attribute for a domain registration from an investigation, high-confidence data feed, or direct observation.
2) Access RDS or other system to build list of domains based on reverse whois lookups on unique elements.
3) Examine list of domains for the same abusive behavior or indicators that they may have been or will be used in a similar matter
4) Use the gathered data to again pivot on unique elements found within the newly discovered domains.
5) Use an investigatory tool like a relationship visualization system to "cluster" domains that have paths of relationships to look for patterns, key elements, and potential clues as to how the miscreant may create new domains in the future.

Use this information to inform other processes like mitigation or criminal investigations.Users: Law enforcement personnel, security researchers, CERT teams, first responders

Data: Full available contact information for registrant and any other contacts (e-mail, phone number, and contact handle most useful), nameservers, registrar, reseller, creation date

1C-3 Purpose Name: Find potentially compromised domains related to an existing hijacking or domain shadowing incident

NEW VERSION: Access information held on a domain name to enable security professionals and law enforcement to find potentially compromised domains related to an existing hijacking or domain shadowing incident.

Definition: When miscreants take over domain names in hijacking or domain shadowing attacks, they often will take over entire groups of domain names due to vulnerabilities in registrar systems, systemic use of weak or compromised passwords, or getting ahold of a

domain portfolio. When one such domain is identified, understanding the scale of the compromise and potential compromise is important to determine as soon as possible to mitigate a larger issue. Miscreants will often change elements of domains involved in such attacks to common infrastructure such as nameservers or update admin or registrant contacts to include new information to allow the miscreant control of the affected domains. Understanding the new and original information for such domains allows investigators and first responders the opportunity to mitigate all domains and not just the reported one(s). This purpose also is greatly enhanced with the existence of "who was" type services that provide historical information on how a domain name was previously listed in an RDS. Such systems are currently run by third parties, and they have been proposed for a future RDS or to be allowed under the framework of a future RDS but those ideas have yet to be explored by the working group.

Tasks:
1) Identify a hijacked or shadowed domain name.
2) Access the RDS to determine current attributes for the affected domain including nameservers, admin and registrant contact details, registrar, registrar abuse contact, and modification date. Admin contact information is vital in case of a hijacking since transfers are usually controlled via the admin e-mail address.
3) Access historical records for the affected domain to obtain the same information. Particularly important is prior registrar in case of a hijacking that involved a domain name transfer.
4) Build list of domains based on reverse whois lookups on key unique elements that have been modified for the domain.
5) Examine list of domains for the same abusive behavior or indicators that they may have been or will be affected in a similar matter
6) Enter notification/mitigation phase with the affected registrar(s) and legitimate registrant.

Users: Security researchers, CERT teams, first responders, registrar abuse teams
Data: nameservers, full admin and registrant contact details, registrar, registrar abuse contact, and modification date.

Subsection 1D: Automatically scoping infrastructure involved in issue

1D-1 Purpose Name: Automatically expand knowledge from one or more known malicious domains to other domains potentially part of the same issue

NEW VERSION: Access information held on a domain name to enable automated security systems to expand knowledge from one known malicious domain to other domains potentially part of the same issue.

Definition: Automatically investigate key attributes of a known malicious domain to find others that may be part of the same or related incidents. This is the same purpose as 1C-1 except at scale, so the data elements involved will typically be more narrowly constrained (typically

nameservers and key e-mail addresses) to allow for fully automated processing. Since criminals/abusers often re-use common elements for registering malicious domains, once a domain has been identified as being malicious, researchers can configure automated processes to take key unique elements from that domain and search for other domains sharing those elements. Such unique elements often include unique nameservers, unique contact data – particularly registrant and/or admin contact e-mail or to a lesser extent, phone number. This purpose requires the existence of some sort of "reverse whois" capability where an RDS, cached database, or third party collection of RDS data can be queried on an attribute and return a list of all domains sharing that attribute. Such domains tend to cluster on less unique elements such as creation date, registrar, and reseller, but using these data elements requires other meta data for correlation. Lists of suspect domains may then be automatically probed to see if they exhibit the same illegal/abusive behavior.

Tasks:
1) Obtain a positively identified malicious domain from prior investigation, trusted data feed, or other high-confidence source.
2) Query RDS for key attributes that allow for "pivoting" to other potentially related domains. Such information will include nameservers, full contact data for registrant, admin, and in some cases tech contacts (particularly unique elements like contact handle, e-mail address and phone number), and other more loosely associable elements like registrar, reseller, and creation date.
3) Determine veracity of supplied information as an informative element. Accurate data is not necessary in this step since repeated bogus data is a strong indicator of associated abuse.
4) Build list of domains based on reverse whois lookups on unique elements.
5) Examine list of domains for the same abusive behavior or indicators that they may have been or will be used in a similar matter
6) Use the gathered data to again pivot on unique elements found within the newly discovered domains.
7) Use an investigatory tool like a relationship visualization system to "cluster" domains that have paths of relationships to look for patterns, key elements, and potential clues as to how the miscreant may create new domains in the future.
8) Use this information to inform other processes like mitigation or criminal investigations.

Users: Automated processes configured by security researchers and incident response teams.

Data: Full available contact information for registrant and any other contacts (e-mail, phone number, and contact handle most useful), nameservers, registrar, reseller, creation date

Section 2: Notifications
Subsection 2A: Notifications in cases where domain has been compromised

2A-1 Purpose Name: Notify parties responsible for a domain name that has had its website compromised

Template for defining an RDS Purpose:
Criminal Investigation or DNS Abuse Mitigation

NEW VERSION: Access information held on a domain name to enable security professionals and law enforcement to notify parties responsible for a domain name that has had its website compromised.

Information collected to enable contact between the registrant and <who> <to accomplish what>

Definition: Internet security personnel, law enforcement and other investigators working on criminal or abuse issues need to inform those parties responsible for a domain name of malicious activities and potential exposure of PII or other information related to a compromised website. These notices will lead to mitigation of the compromise and gathering of evidence related to the malicious activities related to the compromised website.
Tasks:
1) Query RDS for relevant information about contacts for the domain name that has had its website compromised. These contacts would typically include the technical contact (often the web host), registrant (owner), and admin contact (up-to-date responsible party) for the domain.
2) Evaluate the information returned to determine if actual contact data is included, or if it is bogus or privacy protected to prioritize contacts towards actual people or well-defined roles.
3) Attempt to contact responsible parties in real time.
4) Obtain information from contactable contacts to reach actors who can mitigate issues and/or provide evidence/information
5) Work with actors who can take action to mitigate issues and deliver information/evidence.
Users: Law enforcement personnel, security researchers, CERT teams, first responders
Data: Contact information for technical, registrant, and admin contacts including name, phone number, and e-mail address to facilitate notifications and communications.

2A-2 Purpose Name: Notify parties responsible for a domain name that has had its domain management account compromised

NEW VERSION: Access information held on a domain name to enable security professionals and law enforcement to notify parties responsible for a domain name that has had its domain management account compromised.

Definition: Internet security personnel, law enforcement and other investigators working on criminal or abuse issues need to inform those parties responsible for a domain name of malicious activities and potential exposure of PII or other information related to a take-over of a domain name management account. These notices will lead to mitigation of the account compromise and gathering of evidence related to the malicious activities related to the compromised domain. In these circumstances, currently listed contact records may be false due to miscreant capability to modify these entries.
Tasks:
1) Query RDS for information about contacts for the domain name that has been taken over via the domain management account. These contacts would typically include the technical

contact (often the web host), registrant (owner), and admin contact (up-to-date responsible party) for the domain. However, these may not be reliable since the miscreant may have changed them. Registrar abuse contact becomes primary contact to use if this is likely.
2) Evaluate the information returned to determine if actual contact data is included, or if it is bogus or privacy protected to prioritize contacts towards actual people or well-defined roles.
3) Determine if contact information is still reliable. Historical or certified contact information of some sort would be useful in this scenario, if it existed.
4) Attempt to contact responsible parties in real time.
a. At a minimum, make sure registrar is aware of the compromised account and takes action to ensure miscreant cannot re-compromise.
5) Obtain information from contactable contacts to reach actors who can mitigate issues and/or provide evidence/information
6) Work with actors who can take action to mitigate issues and deliver information/evidence.
Users: Law enforcement personnel, security researchers, CERT teams, first responders
Data: Registrar abuse contact primary contact point. Others, if not changed as part of incident, include contact information for technical, registrant, and admin contacts including name, phone number, and e-mail address to facilitate notifications and communications.

Subsection 2B: Notifications in cases where domain has been registered maliciously

2B-1 Purpose Name: Notify registrar and/or reseller of malicious domain name registration for mitigation and/or evidence gathering

NEW VERSION: Access information held on a domain name to enable security professionals and law enforcement to notify registrar and/or reseller of malicious domain name registration for mitigation and/or evidence gathering.

Definition: After an investigator has positively identified a malicious domain registration, they may take further action depending upon their goals. In most cases the goal will be to get the domain suspended or removed from the DNS and prevented from being re-activated by the miscreant. In some cases, the investigator will be looking to obtain information from the registrar, or reseller if applicable, about how the domain was registered including items like payment details, IP address of any online order, or data behind a proxy registration.
Tasks:
1) Determine that a domain name is malicious via an investigation.
2) Access RDS data to obtain official abuse contact information for a registrar or information on involved reseller. Access other resources like a registrar website to get e-mail/phone for abuse desk, customer support or other relevant departments.
3) Evaluate the information returned to determine if actual contact data is included, or if it is bogus or privacy protected to prioritize contacts towards actual people or well-defined roles.
4) Establish communication with registrar and/or reseller if applicable.
5) Request actions including suspension, deletion or transfer of malicious domain name, and/or further information about the actor who registered the malicious domain. In particular,

evidence/information sought out will be about how the domain was registered including items like payment details, IP address of any online order, or data behind a proxy registration.

6) Registrar or reseller takes some sort of action to the request.

7) Escalate to registry if registrar unresponsive or refuses to take action.

Users: Law enforcement personnel, security researchers, CERT teams, first responders

Data: Registrar abuse contact primary contact point. If not available, whatever contact information is available for the registrar. If reseller involved, contact information for the reseller. E-mail address and/or phone number for these contacts is necessary. If escalation to registry is required, abuse contact information for the registry.

Subsection 2C: Automated notifications of abuse

2C-1 Purpose Name: Automatically notify affected parties of abuse issues

NEW VERSION: Access information held on a domain name to enable automated security systems to automatically notify relevant parties associated with affected domain names about abuse issues.

Definition: Some actors who process large volumes of abuse (e.g. spam, botnets) provide automated reporting to affected entities. One of those processes is providing automated reports to registrars and registries of maliciously registered domain names. Their goal is usually to get the domains they have identified suspended or removed from the DNS and prevented from being re-activated by the miscreants who registered them.

Tasks:

1) Determine that a domain name is malicious via a standardized investigatory process and automation..

2) Access RDS data to obtain official abuse contact information for a registrar or information on involved reseller. Access other resources like a registrar website or abuse reporting API.

3) Access RDS to obtain relevant information for domains being reported to include with report so registrar/registry/reseller can locate other domains with the same attributes and potentially take action.

4) Use e-mail, abuse reporting API or whatever listed contact information is available to establish communication with registrar and/or reseller if applicable.

5) Report relevant RDS information that may indicate miscreant activity and request actions including suspension, deletion or transfer of malicious domain name.

6) Registrar or reseller takes some sort of action on the request.

7) Escalate to registry if registrar unresponsive or refuses to take action.

Users: Security researchers, CERT teams, first responders

Data: Registrar abuse contact primary contact point. If not available, whatever contact information is available for the registrar like an abuse reporting form or API. If reseller involved, contact information for the reseller. E-mail address and/or phone number for these contacts is necessary. If escalation to registry is required, similar abuse contact information for the registry. Reported information will typically include registrant name, e-mail, admin e-mail, phone numbers for registrant and admin contacts, and nameservers.

Template for defining an RDS Purpose:
Criminal Investigation or DNS Abuse Mitigation

Section 3: Determine Reputation

3A-1 Purpose Name: Automatically create reputation score for domain names

NEW VERSION: Access information held on a domain name to enable automated security systems to automatically create reputation score for domain names.

Definition: Calculate a reputation score for a domain name that represents a scalar value or set of values for the relative risk for engaging in different communications for a domain. Publish these scores for subscribers who will make decisions on operations like e-mail delivery, network connections, web browsing requests, and other data exchanges. This includes the use of fixed algorithms on subscriber networks as well as updating scoring metrics by the reputation provider. Scoring processes usually take into account abuse reports and white lists to better classify domains or domain elements like nameservers or registrar.

Tasks:

1) Deploy a domain reputation scoring algorithm based on prior work and investigations into various forms of malicious and benign domain names. Modern systems use machine-learning for a majority of these tasks.
2) Receive a new domain name to score or a previously seen one to update from one of many processes. Inputs in this step include parsing new domains out of daily zone files, observations in passive DNS sensor networks, subscriber requests based on observed connection attempts.
3) Access RDS to obtain key elements required 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.
4) Obtain other meta data from other sources to improve scoring including abuse reports, other reputation lists, lists of known DGA (domain generation algorithm) domains, “allow” lists, and known benign infrastructure.
5) Score domain name and publish score in file, feed, or as a query response.
6) Update algorithm, algorithm parameters, and/or domain element knowledgebase using new information obtained in processing recent domain scores.

Users: Automated processes and researchers working for organizations that provide reputation scores for domain names

Data: Creation date, expiration date, nameservers, registrar, contact information for technical, registrant, and admin contacts including name, phone number, and e-mail address

Template for defining an RDS Purpose:
Criminal Investigation or DNS Abuse Mitigation

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-CrimInvAbuseMit10%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 RDS Purpose:

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

Template for defining an RDS Purpose:
Criminal Investigation or DNS Abuse Mitigation

RDS Purpose: Criminal Activity or DNS Abuse Notification

DT7 Answers to Questions – First Draft for DT Review Criminal Activity/DNS Abuse Mitigation – Notification From https://community.icann.org/download/attachments/74580010/DraftingTeam7-CrimInvAbuseMit10%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.

Template for defining an RDS Purpose:
Criminal Investigation or DNS Abuse Mitigation

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-CrimInvAbuseMit10%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.

Template for defining an RDS Purpose:
Criminal Investigation or DNS Abuse Mitigation

ICANN61 F2F 14 March 2018 WG Notes

DT7 Criminal Investigation/DNS Abuse Mitigation Investigation, Notification, and Reputation

- Answers introduced by Marc, noting limited participation of DT7 members in drafting answers
- Overall there are two paths: investigate a possible criminal or contact a possible victim
- During investigation, the entity to be identified is whomever is controlling the DN – that may not be the rightful owner of the DN
- During investigation, may also be appropriate to contact the registrar, reseller, or privacy/proxy provider to identify the possible criminal engaged in the activity or abuse
- During notification, the primary objective is to inform the possible victim; the secondary objective is enabling mitigation of the activity/abuse
- Page 1 Question 2 of DT7 answers: Objective should include reputation?
- How is Question 3 helpful for this purpose? May describe any obligation on response (or lack thereof). May also describe possible benefits to data subjects.
- Were these definitions informed by jurisdiction and limitations imposed by laws in certain jurisdictions? No – application of purposes would depend on jurisdiction and policy, which the drafting team considered outside its remit when simply describing the purpose
- Criminal activities should also include hate crimes, infringement of civil liberties, etc. – these should be noted to ensure consideration during deliberation of this purpose
- What constitutes criminal activity varies from one jurisdiction to another
- For example, blasphemy vs. freedom of speech
- What kinds of activities should be pursued through this purpose vs. who should have access to data for this purpose vs. consent given to collect data for this purpose
- This purpose should focus on providing a mechanism to be used in jurisdictions, for activities, where it is appropriate
- What do we do when law enforcement is “bad” and criminal activity is “good”?
- Being able to notify a registrant that their DN has been compromised is clearly useful
- Being able to use reputation scores to deter abuse and crime is good
- Where we disagree is in use of registration data to investigate criminal activity
- Legal processes for accessing data for this purpose will be determined by laws, not policy
- For clarity, this purpose should be titled “Criminal Activity Mitigation and DNS Abuse Mitigation” (or Investigation of Criminal Activity and DNS Abuse, Notification of…, etc.)