

User Story:

	User Type	Data Elements	Purpose Specification	Other Info
1	<b>As a [Insert User Type from list]</b>	<b>I use the following data elements: [insert from list, add anything missing]</b>	<b>For the purpose of [specify]</b>	<b>Any other relevant data</b>
2	Potential registrant	Domain name, registrar, deletion date	Determine if domain name is available for registration	
3	Registrant –creating an account at a registrar and registering a domain name	Business account information, Billing information, Domain name information which includes: Name of Registrant, email address, name servers, postal address, phone number, Admin and technical contact, servers, creation date, expiration date. Payment information	Domain Name Registration	
4	Registrant, Registrar,		Domain Name Maintenance	
5	Registrant, Registry, gaining registrar, losing registrar, reseller	Transfer EPP key, domain status, domain creation date and expiry date, admin contact email address, nameservers/DNS records.	Domain name maintenance - Transfer Domain	Registrars will need to collect 4 key pieces of information to effect a domain transfer, in addition the account and billing information details.

				<ol style="list-style-type: none"><li>1. The registrant needs to provide the gaining registrar with a <b>valid EPP (transfer authorization code)</b> which is issued by the losing registrar. The gaining registrar validates this EPP key with the losing registrar.</li><li>2. The gaining registrar will check that the <b>domain status</b> is "ok" or unlocked for transfer.</li><li>3. The gaining registrar will check that the domain is not past <b>expiry</b>, and the <b>creation date</b> is greater than 60 days old.</li></ol>
--	--	--	--	--

				<p>4. The gaining registrar will send a transfer authorization email to the listed <b>email address for the admin contact</b> on the whois. This can be obfuscated eg. by whois privacy, or incorrect details provided at registration</p> <p>The domain transfer will complete once all above conditions have been met and the transfer authorization email has been accepted. Please see an example below.</p>
6	Registrant, registrar, registry	Domain status, expiration date	Domain name maintenance - Deletions	<p>To detect when a lapsed domain is due to drop they can check the expiry date and the domain's status. Using this information they can tell when it will drop.</p>

7	Registrant, registrar	Registrar information, Nameserver entries	Domain name maintenance - DNS Changes	Changing a domain's DNS records
8	Registrant, registrar, billing contact	domain status, domain expiry date, billing details, renewal period in years.	Domain name maintenance - Renewal	Renewing a registered domain name.
9	Registrant, registrar, registry	Statuses	Domain Name status monitoring	Monitoring unauthorized changes in statuses of high value domain names.
10	Registrant, registrar	Domain name, registrant, address, phone number, email address, admin, address, phone number, email address, tech contact, address, phone number email address, registrar information, nameservers, statuses, renewal date, expiration date	Domain Name Portfolio Management	Domain Name manager reviews all data elements in whois records for accuracy.
11	Registrant, Registrar, third party, broker	Name of Registrant, email address, postal address, phone number, company registration number/trading name	Domain Buyer Broker	Domain broker is seeking to confirm if the online retailer is a valid trading entity and if it has made genuine trading filings in the last 3 years. Ideally, broker will seek to obtain a copy of the retailer's company information, approximate

				<p>book value and company filings. Identify who the registrant is and his postal address. Cross reference this against the local company registrations service to identify the relevant business. Determine through the company information if the retailer's counteroffer is justifiable on the basis of financial information.</p>
12	<p>Business interested in acquiring a domain name registration, registry, registrar and third party WHOIS service providers</p>	<p>: Name of Registrant, email address, name servers, postal address, phone number, creation date, servers last update.</p>	<p>Domain name acquisition</p>	<p>When branding new products or services most companies will want to register a .com domain name to insure there is not a competing service or product on the web. To acquire a domain name research in to the history of the domain name is essential. Using the current WHOIS information searches are conducted to insure that the current registrant has clear right to sell the domain</p>

				name. Also research into the previous use of the domain name and other domain names the registrant owns
13	<p>Company Buyer or Seller or Agent (e.g., Law Firm or Accountancy Firm that might be handling due diligence)</p> <p><b>Other Stakeholders:</b> Operator of the DNS, registrant, registrar</p>	Name/Organization, Location (address details), registration date/status, possibly email (if looking to run a Reverse Whois)	<p>Asset Verification</p> <p>Merger / Spinoff (to be merged with) M&amp;A</p> <p>Target Portfolio Analysis</p>	<p>NewCo is seeking to buy Company A and spinoff a division to Company B. NewCo needs to verify: 1) the domains that are owned by Company A, and 2) the information on domains Newco owns that it intends to sell to Company B. It needs to run a Reverse Whois search to determine what other domain names are owned by Company A that was not disclosed to NewCo, Simultaneously, Company B needs to verify the domains that are owned by NewCo. Company B also needs to run a Reverse Whois search to determine what other domain names are owned by the NewCo division that were not disclosed to Company B.</p>

14	<p>Person experiencing a technical issue with a registered domain name.</p> <p><b>Other stakeholders:</b> Operator of the gTLD Directory Service for the queried domain name, person, role, or entity associated with the registered domain name who can resolve technical issues, registered domain name registrant (who may care to know about operational issues), registered domain name registrar or hosting provider (who may be providing an operational service), proxy service provider (who may be providing a proxy service for the person, role, or entity associated with the registered domain name who can resolve technical issues).</p>	<p>Data elements that allow communication in real or near-real time are the most useful in the context of this use case. These include an email address, an instant messaging address, a telephone number, and/or an indicator that identifies the preferred contact method specified by the registrant. Section 4 of RFC 2142 describes recommendations for abuse@, noc@, and security@ email addresses to “provide recourse for customers, providers and others who are experiencing difficulties with the organization’s Internet service”, but it is important to note that the public nature of these addresses often makes them attractive to unsolicited bulk email senders.</p>	Technical Issue Resolution	<p>A person experiences an operational or technical issue with a registered domain name. They want to know if there’s someone they can contact to resolve the problem in real or near-real time, so they use a tool to look for information in an online gTLD Directory Service to identify an appropriate person, role, or entity that possesses the ability to resolve the issue. An incomplete list of examples of technical issues includes email sending and delivery issues, DNS resolution issues, and web site functional issues.</p>
15				
16	Researcher	Domain Name Registrant Name	Research/statistical	A researcher wants to perform statistical analysis

	<p><b>Other stakeholders:</b> Operator of the DNS, registrants of each domain name, registrars for each domain name, organization sponsoring study (e.g., ICANN, SO/AC, registry, third party)</p>	<p>Registrant Organization  Registrant Type (Natural or Legal Person or Proxy)  Registrant Unique Identifier (for aggregation and/or for querying other databases)  Registrant Postal Address (for geographic analysis and/or postal survey)  Registrant Email Address (for geographic analysis and/or email survey)  Registrant Phone Number (for geographic analysis and/or phone survey)  Registrar Name (for provider analysis and/or registrar survey)  Registration Date/Status (for temporal analysis)  Domain Name Purpose (Commercial, Non-Commercial, other)</p>	<p>analysis</p>	<p>or conduct a study about gTLD domain name registration or usage or benchmark related processes. Study goals and methods vary, but many studies about gTLD domain names begin by creating a sample of names to be studied, then using a directory service to obtain registration data associated with those names.</p>
17	<p>Service Provider (e.g Registrar, web hosting companies) seeking alternate contacts information for a customer (registrant) whose known contact information becomes invalid.</p>	<p>Data elements that are useful in this use case can be real-time like phone, IM etc or non real time like email, postal etc.</p>	<p>Service Provider Contacting Registrant (</p>	<p>A service provider (registrar, web hosting company) is having trouble sending bills to a customer (registrant of a domain name). The customer's email with the</p>



	<p><b>Other stakeholders:</b></p> <ol style="list-style-type: none"> <li>1. Operator of the gTLD Directory Service for the queried domain name, person,</li> <li>2. Role, or entity associated with the registered domain name (eg Technical contact) who can provide valid billing email address,</li> </ol> <p>Proxy service provider (who may be providing a proxy service for the person, role, or entity associated)</p>			<p>service provider bounces back when bills are sent by email. The service provider does not want to cancel the customer's account and loose this customer on the basis of invalid contact. The service provider makes extra effort to find out if there are alternative ways of reaching the customer. He goes to an online gTLD Directory Service to seek alternative contacts for the customer or other contacts, eg technical contact for the domain, that could assist in the effort to reach the customer.</p>
18	<p>Website endusers and consumers</p> <p><b>Other stakeholders:</b> registry, registrar and third party WHOIS service providers</p>	<p>Name of Registrant, email address, postal address, phone number, company registration number/trading name</p>	<p>Consumer Protection</p> <p>Contact Online Retailer to Resolve Issue</p>	<p>A consumer/domain name end-user uses WHOIS information to source contact information for an online retailer, having failed to secure an adequate point of contact on the website itself</p>

19	<p>Automated process running on system(s) of an authenticated user of the DNDS system that is obtaining information related to domain name(s) or domain name attributes.</p> <p><b>Other stakeholders:</b> Operator of the DNDS, registrant of queried domains, any listed contacts returned by querying the system, registrar/reseller of queried domains, providers for Internet services (web/e-mail/messaging/etc.) for the domain name.</p>	<p>Nameservers assigned to the domain names identified  e-mail addresses used to control the domain(s)  registrar(s)/reseller(s) of domain names identified  Domain registration/renewal date  Domain status  contact info associated with the domain name  - Name/Org Name  - e-mail address  - phone  - physical address</p>	<p>Reputation Services</p>	<p>Automated reputation system (process) receives domain name or domain name components to evaluate or update. Process accesses the DNDS via established access methodology and authentication credentials. Process queries about one or more domain names to retrieve full information about the domain name(s) entered. If the starting point is a particular domain attribute like a nameserver or e-mail address, the DNDS will create a list of domains with those attributes. Based on the results obtained, the DNDS returns a list of domain names and potentially other information the process is entitled to given its credentials. The process then applies algorithms typically based on stored reputation data to assign</p>
----	--	--	----------------------------	--

				reputation values/scores to the domain name or domain name attributes being scrutinized. The process will likely iterate on this case many times based on the information various searches reveal.
20	<p>Certificate Authority</p> <p><b>Other stakeholders:</b> Registered domain name registrant or entity operating on behalf of the registrant, operator of the gTLD Directory Service for the queried domain name, registered domain name registrar or hosting provider (who may be providing an operational service to generate a CSR or provide a proxy service), proxy service provider, Certification Authority.</p>	<p>Data elements that uniquely identify the certificate Applicant are the most useful in the context of this use case. At the low end of the certificate service scale these include items that can be validated in near-real time through direct contact, such as an email address, an instant messaging address, and a telephone number. At the higher end of the certificate service scale this would include personal names, an organization name, and a postal address.</p>	Certification Services	<p>An Applicant contacts a person or automated process associated with a CA with a request to create a digital certificate that is bound to a domain name. The CA asks the applicant to provide the domain name in the form of a Certificate Signing Request (CSR). The CA retrieves and decodes the CSR and accesses an online resource for displaying contact information associated with registered domain names under a TLD or TLDs. The CA submits the domain name to the online resource for processing. The resource</p>

				<p>returns information associated with the domain name that includes entities that can be contacted and entity metadata that can be validated to confirm the identity of the Applicant. The CA then uses the retrieved information (sends email to the registrant or technical contact email address and waits for a reply, compares address information to public records, etc.) to confirm that the Applicant has the exclusive right to use the specified domain name. The certificate generation process typically fails if the information provided by the Applicant cannot be matched to information published in the Directory Service.</p>
21	<p>Brand owner</p> <p><b>Other stakeholders:</b> registry, registrar and third party</p>	<p>Name of Registrant, email address, name servers, postal address, phone number, creation date, expiration date</p>	<p>Regulatory/licensing</p>	<p>A government entity is requesting information about our online business. We need to show which</p>

	historical DNS service providers, tax authority			entity currently is the registrant of the domain name, the registrant history of the domain name once we acquired it and when we registered, recovered or acquired it.
22	Brand Owner  <b>Other stakeholders:</b> registry, registrar and third party WHOIS service providers <b>Scope:</b> Interacting with Domain Name Directory Service	Name of Registrant, email address, name servers, postal address, phone number, creation date, servers last update.	Fraudulent and inaccurate info	Inaccurate information intentionally used in the WHOIS record– the information in the WHOIS is a blatant attempt to make it appear that the registration is owned and controlled by a target company. Domain name involved in a variety of fraudulent uses
23	: Consumer  <b>Other stakeholders:</b> Directory service provider (e.g., registry, registrar, or other) website registrant	registrant: name, address, and contact details	Real World Contact	A query for replacement parts is performed by inputting known grill information into a search engine. Consumer is then presented with search results displaying numerous websites with low price alternatives for replacement parts. Some of the websites are not famous brand-name

				<p>retailers, and the consumer must try to determine the validity of the websites he/she may transact with. Real World Information as one method for establishing a trusted online transaction. When engaging in online transactions, consumers can use directory services to, at a minimum, compare the registration data to what is seen on the website (e.g., Amazon.com, displaying the brand AMAZON, is owned by a company called Amazon based in Washington – known to the consumer). This type of comparison is a good tool to help consumers determine the validity of the websites they may transact with online.</p>
24	<p>ICANN Contractual Compliance</p> <p><b>Other stakeholders:</b> Registrant, ICANN, and Complainant</p>	<p>all data fields pertaining to the registrant, admin, tech, and billing contacts, in addition to the domain registrar, status, nameserver,</p>	<p>Contractual Compliance Contact</p>	<p>Enforcement of registrar and registry contractual obligations under the RAA and registry agreements</p>

		update date, creation date, and expiration date.		requires access to registration data under various scenarios.
25	<p>Random illicit actor</p> <p><b>Other stakeholders:</b> registrar, targeted websites, end-users</p> <p><b>Scope:</b> Interacting with a registrar</p>	Registrar information, NameServer entries	Domain Name Hijack	Malicious use of information of a domain name in WHOIS in an attempt to hijack the domain name.
26	<p>Spammers, scammers, or criminals (miscreants) who desire to send messages to entities associated with domain names and/or find “working” contact information, particularly e-mail addresses.</p> <p><b>Other stakeholders:</b> Operator of the DNDS</p>	<ul style="list-style-type: none"> <li>- Name/Org Name</li> <li>- e-mail address</li> <li>- phone</li> <li>- physical address</li> </ul>	Mining data for spamming/scamming	Spammers, scammers, and various criminals (miscreants) desire to send messages to entities associated with domain names and/or find “working” contact information, particularly e-mail addresses. Miscreants use this information to contact potential victims for various scams like phishing, computer intrusions, confidence scams, etc. While spam is the most prevalent method used today, phone numbers are harvested for both SMS and

				<p>direct calls, and physical addresses are used for mailing fake notifications (e.g. fake domain renewal notices) or other scams. Some miscreants tie data available from the DNDS to create targeted attacks against organizations, including domain name hijacking attempts</p>
27	<p>Person intent on using domain names for cimrinal/abusive purposes (miscreant)</p> <p><b>Other stakeholders:</b> Registrar (reseller if applicable) of malicious domain, Registry of the malicious domain, Operator of the DNDS</p>	<p>Nameservers assigned to the malicious domain name(s)</p> <p>registrar(s)/reseller(s) of domain(s) contact info used by the miscreant</p> <ul style="list-style-type: none"> <li>- Name/Org Name</li> <li>- e-mail address</li> <li>- phone</li> <li>- physical address</li> </ul> <p>Stolen/fraudulent payment credential details</p> <p>Cracked domain management account details – username/password/multi-factor tokens</p>	Malicious Domain Name Registrations	<p>Person intent on using domain names for cimrinal/abusive purposes (miscreant) selects a registrar and creates or accesses existing domain name registration account.</p> <p>Scenario 1: Miscreant utilizes stolen payment credentials (e.g. purloined credit card information) to create and pay for new domain name registration(s)</p> <p>Scenario 2: Miscreant uses an existing legitimate, but compromised domain name</p>



				<p>management account to create a new domain name registration(s)</p> <p>Scenario 3: Miscreant uses an account at a “black hat” domain registrar/reseller in order to create a new domain name.</p> <p>Miscreant then uses the domain name to support the criminal;/fraudulent/abusive purpose they have in mind.</p> <p>Registrar of record enters the domain into the worldwide DNS and DNDS.</p> <p>This malicious domain remains active in the worldwide DNS until the registrar or registry for that domain receives complaints, uncovers the fraudulent registration, or payment fails.</p>
--	--	--	--	---

				The registry or registrar then suspends or deletes the malicious domain.
28	<p>Botnet masters (miscreants) who utilize domain generation algorithms (DGAs) in their bot code to seek out ever-changing C&amp;C domains for further instructions, which the miscreants register to control their botnets, and monitor to see if others have reverse-engineered their malware and are pre-registering domains; Law enforcement and operational security personnel (investigators) searching for DGA domains, miscreants, and other investigators.</p> <p><b>Other stakeholders:</b> Registrar (reseller if applicable) of malicious domain(s), Registry of malicious domain(s), Operator of the DNDS</p>	<p>Nameservers assigned to the malicious domain name(s) registrar(s)/reseller(s) of domain(s) contact info used by the domain registrant (potentially miscreant or investigators)</p> <ul style="list-style-type: none"> <li>- Name/Org Name</li> <li>- e-mail address</li> <li>- phone</li> <li>- physical address</li> </ul>	Malicious Domain Generation Algorithms	<p>LE/Ops-Sec type person (investigator) accesses the DNDS via their credentials. The investigator enters one or more domain names that are calculated to be used by a domain generation algorithm (DGA) over some period of time. The system returns a list of domain names and potentially other information the investigator is entitled to given their credentials. The investigator may iterate on this case many times based on the information various searches reveal. The investigator uses this information to investigate the operations and potential miscreants behind a DGA based botnet, perform notification and mitigation activities, and</p>

				<p>identify other investigators and mitigation efforts.</p> <p>Alternatively, a botnet operator (miscreant) accesses the DNS via their credentials. The miscreant enters one or more domain names that are calculated to be used by a domain generation algorithm (DGA) over some period of time. The system returns a list of domain names and potentially other information the miscreant is entitled to given their credentials. The miscreant will use this information to monitor for investigators pre-registering domains so they can update their algorithms and botnet malware as needed.</p>
29				
30				

