Request for Information
on
Contact Data
Validation and Verification Systems

7 February 2014

Internet Corporation of Assigned Names and Numbers
Request for Information

1.0 Introduction

1.1 About this Document

By issuing this Request for Information ("RFI"), the Internet Corporation for Assigned Names and Numbers ("ICANN"), is requesting information related to commercially-available services and software that might be capable of validating or verifying domain name registration contact data.

This RFI is intended to inform two distinct ICANN projects that require address validation and verification.

The first project is related to a near-term need for postal address cross-field validation services arising out of requirements applicable to those registrars who have signed the new 2013 Registrar Accreditation Agreement (referred to herein as the RAA Project). The requirements related to the RAA Project are described in greater detail in Section 2 of this RFI.

In addition, ICANN is seeking similar information for a separate longer term project in connection with Expert Working Group on Next Generation gTLD Directory Services ("EWG") recommendations to identify a replacement to the current WHOIS system. The EWG is now developing recommendations for a new system that could better meet global Internet community needs for domain name registration data while offering greater privacy, accuracy, and accountability (referred to herein as the EWG Project). The requirements related to the EWG Project are described in greater detail in Section 3 of this RFI.

As the purpose of this RFI is purely informational – that is, to inform the development of policies and procedures -- potential Respondents responding to the future RFP (if any) will not be bound by the estimates, prices, or other information provided in response to this RFI. Similarly, there is no obligation on the part of parties responding to this RFI to submit a future RFP bid, or for ICANN to proceed to RDS implementation or vendor selection, with or without issuing a future RFP.

1.2 Overview of ICANN

The Internet Corporation for Assigned Names and Numbers (ICANN) is an internationally organized, non-profit corporation responsible for coordinating critical Internet resources. These include Internet Protocol (IP) address space allocation, protocol identifier assignment, generic (gTLD) and country code (ccTLD) Top-Level Domain Name System (DNS) management, and root server system management. As a private-public partnership, ICANN is dedicated to preserving the operational stability of the Internet; to promoting competition; to achieving broad representation of global Internet communities; and to developing policy appropriate to its

mission through bottom-up, consensus-based processes.

In support of this mission, ICANN develops policy for WHOIS services that provide public access to data about registered domain names. The extent of data collected at the time of domain name registration, and the ways such data can be accessed, are specified in agreements established by ICANN for domain names registered in gTLDs.

For example, ICANN currently requires its accredited registrars to collect and provide free public access to information about each registered gTLD domain name, including the name servers for that domain, the date the domain was created and when its expires, the Registered Name Holder's name and contact information, and designated Technical and Administrative contacts. Today, anyone can obtain this data by using the WHOIS system.

Section 2.0 Additional Information on the RAA Project

2.1 Current Requirements for Address Validation

Registrars who are accredited pursuant to the most current form of RAA (the "2013 RAA") are currently required to perform limited validation of registration contact data. This requirement generally ensures that customers' registration data fit into appropriate forms or conventions. That is, email addresses must conform to RFC 5322, telephone numbers must follow the ITU-T E.164 notation for international telephone numbers, and postal addresses must conform to the Universal Postal Union's S42 templates. The agreement also requires that registrars begin performing cross-field validation of addresses; provided it has been determined that such validation is deemed to be commercially and technically feasible.

2.2 Overview of the 2013 RAA Requirement (cross-field postal address validation)

As noted above, registrars who are accredited under the 2013 RAA are currently required to perform limited validation of registration contact data. The agreement envisions that registrars will also perform cross-field validation of address data (e.g., the house number exists on the street, which exists in the city and province, and the postal code is correct). This cross-field validation requirement becomes effective 6 months after ICANN and a working group of registrar volunteers have agreed that cross-field validation is technically and commercially feasible.

ICANN has convened the registrar working group that is exploring address validation service options. This RFI is intended to help inform that working group's work.

2.3. Objectives of the RAA Project

As described above, ICANN and the working group of accredited registrars are in the process of measuring the technical and commercial feasibility of performing cross-field international address validation for domain name registrations. In particular, ICANN and registrars wish to determine whether address validation services are readily available, in which countries, and the extent to which such services may be feasibly implemented by registrars. ICANN further seeks information to help guide its consideration of whether and to what extent it should be involved in the provisioning of third-party address validation services to registrars.

Section 3.0 Additional Information on the EWG Project

3.1 Possible Future Requirements for Contact Data Validation

In 2013, the Expert Working Group on gTLD Directory Services (EWG) was formed by ICANN's CEO, Fadi Chehadé, at the request of ICANN's Board, to help resolve the nearly decade-long deadlock within the ICANN community on how to replace the current WHOIS system. The EWG's mandate is to reexamine and define the purpose of collecting and maintaining gTLD registration data, consider how to safeguard and improve accuracy and access to that data, and propose a next generation solution that will better serve the needs of the global Internet community.

Please see ICANN's website for more information on the EWG activities, including its initial recommendations for improving registration data accuracy through (among other things) standardized validation practices.

3.2 Overview of the EWG Initiative

In its Initial Report, the EWG recommended a paradigm shift whereby gTLD registration data is collected, validated and disclosed for permissible purposes only, with some data elements being accessible only to authenticated requestors that are then held accountable for appropriate use. The EWG is in the process of finalizing its recommended principles, including those intended to approve accuracy through the validation and verification of various data elements to be collected and displayed by the next-generation Registration Directory Service (RDS).

As stated in its Initial Report, the EWG proposes more robust validation of registrant data than provided by either today's WHOIS system or enhancements that may be achieved through broad implementation of the 2013 RAA. To accomplish this, the Initial Report proposed that the RDS create a standard validation service for all gTLD registration data. In addition to periodic checks, validation would occur at the time of collection, with an option to pre-validate registrant contact data for reuse in multiple domain name registrations. The EWG is still working to flesh out the details of validation and related processes, and the results of this RFI will inform its deliberations as it finalizes its recommendations.

This RFI is intended to solicit responses from commercial providers of services and software that might be capable of meeting some or all verification and validation needs associated with various registration data elements which may be included in the new RDS.

At this juncture, the EWG is seeking information to understand the breadth and depth of data validation/verification solutions that are commercially available, and the degree to which they might be used fulfill gTLD registration data needs, should ICANN pursue RDS implementation. This RFI also seeks to identify potential software/service providers and published or available fee

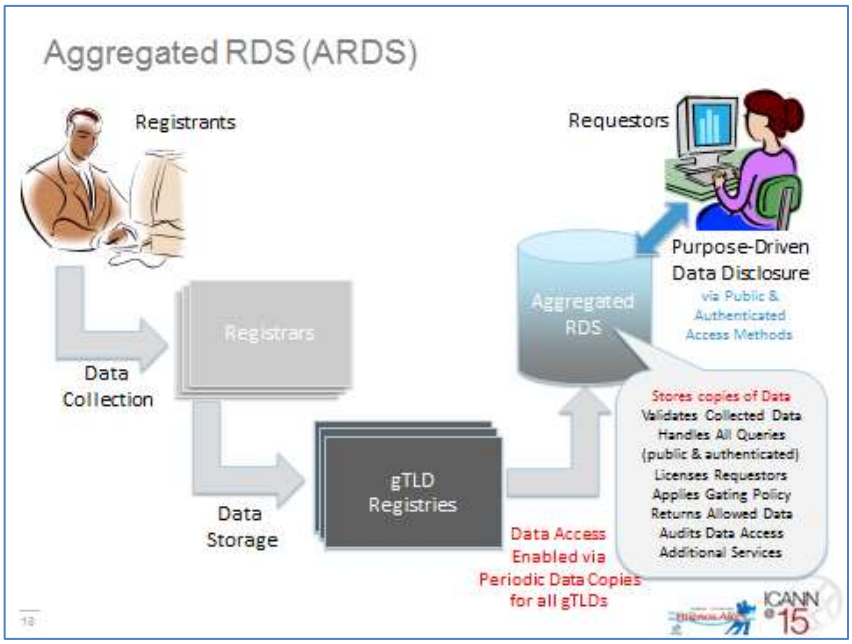
information, to help ICANN assess RDS implementation feasibility and costs. Following a GNSO policy development process (PDP) to be commenced at the Board's request to evaluate the EWG recommendations, the ICANN Board may decide to fund development of a next-generation RDS, and may issue a Request for Proposal (RFP) seeking potential respondents to be considered as a supplier of validation/verification solutions.

3.3 Objectives of the EWG Project

As described above, ICANN may need to engage one or more providers of validation and verification software and/or services to provide cost-effective and timely checks on registration data to be collected and maintained by a new RDS that now under consideration to replace the current WHOIS system.

Currently, there are over 140 million gTLD domain names registered by registrants located all over the world. The RDS is proposed by the EWG to provide centralized access to one or more repositories containing registration data for all gTLD domain names. Under the EWG's proposal, each gTLD domain name would be validated or verified to some degree at the time of registration and periodically thereafter.

The following figure illustrates one of two system models for a next generation RDS that the EWG has identified as having the potential to fulfil many of the principles discussed in the EWG's Initial Report.



Some key features of this proposed RDS that impact data validate/verification include:

- The RDS serves as an aggregated (centralized) or federated (distributed) repository that contains a non-authoritative copy of data elements collected for each registered domain

- Each gTLD Registry remains the authoritative source of that registration data
  - In the Aggregated RDS model, the RDS provides access to cached registration data copied from gTLD Registries and maintained through frequent periodic updates.
  - In the Federated RDS model, the RDS provides access to registration data that is retrieved in real-time from gTLD Registries.
- The RDS (or another third party interacting with RDS, referred to in the EWG's Status Update Report as a "Validator") would be responsible for performing data validation
- The RDS would be involved in handling data accuracy complaints and monitoring compliance with data accuracy requirements, as further detailed in the EWG's Status Update Report

To learn more about the EWG's proposed RDS, watch this short introductory video, listen to this longer presentation, or consult these RDS FAQs. Sections of the EWG's Initial and Status Update Reports describing registration data and validation/verification have been included in Appendix A.

Section 4.0 Requirements of this RFI

4.1 Desired Experience of Potential Respondents for the RAA Project and the EWG Project

Ideally, ICANN expects that potential Respondents to this RFI will satisfy the following experiential requirements:

1. Possess knowledge of the existing WHOIS system and sufficient understanding of the proposed RDS to respond to this RFI.
2. Have a demonstrated ability to handle contact data validation and verification services in an expedited, real-time or near-real-time, robust and reliable manner.
3. Have a track record in competently validating and verifying, and scoring domain name registration data, or for other types of online services, collecting/maintaining similar data elements.
4. Have the ability to potentially onboard hundreds of registrar/validator clients (or a single, centralized high-volume client) and meet the demands of potentially unknown number of new registrations of domain names on a daily basis throughout the world.
5. Be experienced in working internationally, with globally, linguistically, and culturally diverse customers and stakeholders.
6. Have experience and ability to validate or verify data where names or addresses might be represented in non-ASCII scripts.
7. Have a demonstrated understanding of domain name registration issues, including the need for accurate data, timely updates, and policy-driven remediation processes.

4.2 General Service Requirements and Information Requested

Respondents are asked to provide:

1. Their company name, location, and applicable product or service brands.
2. The name/contact details of a person at the company for follow-up purposes.
3. A description of their available services, including:
    a. Quality and sources of comparison data used to verify addresses
    b. Scoring methodology, if applicable
    c. Handling of non-ASCII characters in addresses or supplied data
    d. Robustness / redundancy / geographic diversity of hardware / connectivity, if applicable
    e. A description or example of technical implementation of the service or software

4. A list of the countries for which address validation services are provided, along with the level of precision of validation available.
5. The type of validation or verification that the respondent is capable of performing (Syntactical, Operational, Identity).
6. The general time frame required for each of the validation services to be performed (e.g., n milliseconds/hours/etc.).
7. Known limitations of the validation and verification services that might be relevant to the projects described herein.
8. The relative incidence of errors or false positives (if known), and any process for solving them.
9. Approximate pricing of available validation and verification services or software and commonly-associated terms of usage.

4.3 Specific requests related to the RAA Project

With regard to the RAA Project, Respondents are asked to additionally address the following:

1. Suggested business approach(es) for handling the 2013 RAA's validation requirement by registrars (e.g., arrangements in which every registrar enrolls itself in the address validation service (or a competing AVS), in which the service is "resold" by ICANN , or in which ICANN operates part or all of the AVS service).
2. Any other information that might be relevant to the deployment of such services.

4.4 Specific requests related to the EWG Project

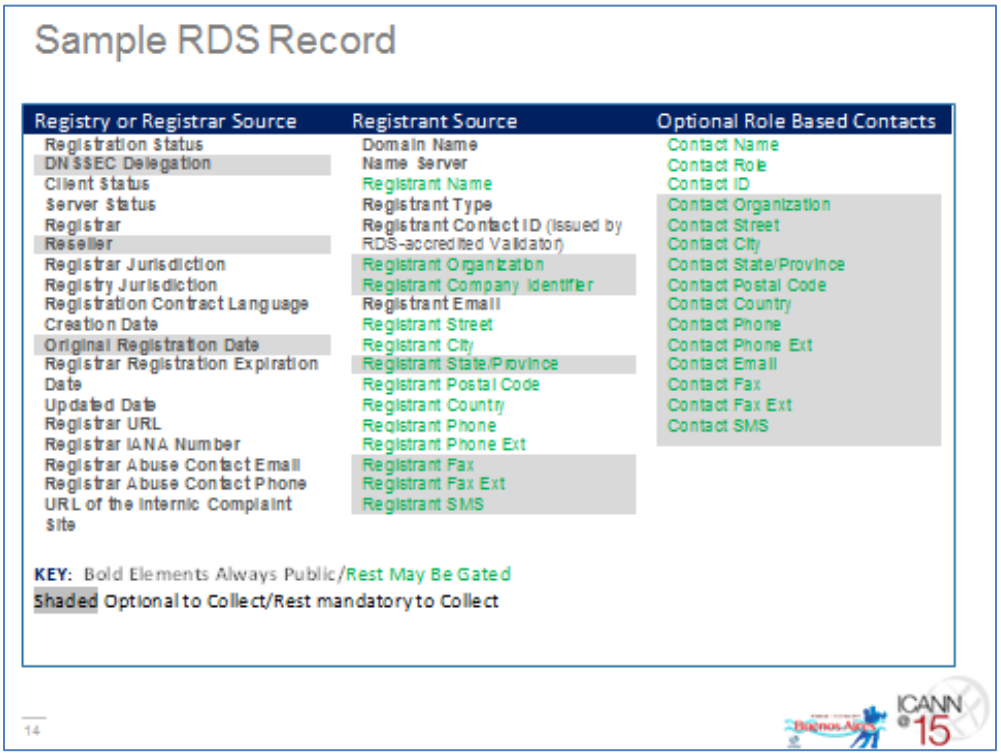
With regard to the Next-Generation Whois recommendations of the EWG, Respondents are asked to additionally address the following:

1. Specific method(s) of implementing the EWG's proposed validation & verification features, including:
    a. Global Postal Address Validation Services
    b. E-Mail Validation Services
    c. Global Telephone Number Validation Services
    d. Global Individual and Business Identity Validation Services
    e. Creation of a Unique Contact Identifier for each Registrant or designated point of Contact that can be reused in multiple domain name registrations
    f. Validation as appropriate for any other data elements proposed to be included in an RDS Record

2. Does your company currently offer services or software that might be used in some fashion to fulfill any of the five features a-f listed in 1) above? If so, please describe the applicable product or service brands, addressing all of the requirements enumerated in section 4.2 and also:
    a. The features, geographic reach, languages available
    b. Whether the service is automated or requires manual intervention
    c. Any other information that might be relevant to the deployment of such commercial services to the RDS

3. Could respondent develop a custom solution to offer any of the five features a-f listed in 1) above? If so, please describe:
    a. The name and location of a company that might be interested in developing the RDS's validation services
    b. Any special expertise that the company has in either the domain name industry (including for ccTLDs), online services generally, or in providing validation services
    c. A brief estimate of the likely costs and time needed to implement the solution (if known)
4. Any other information that might be relevant to the deployment to this RFI?
5. Is there any additional information that should be considered by the EWG as it finalizes its recommendations with respect to the RDS?
6. What issues or concerns do you foresee with respect to validating any o**f the data elements listed** above on a global basis?

A sample RDS record follows:



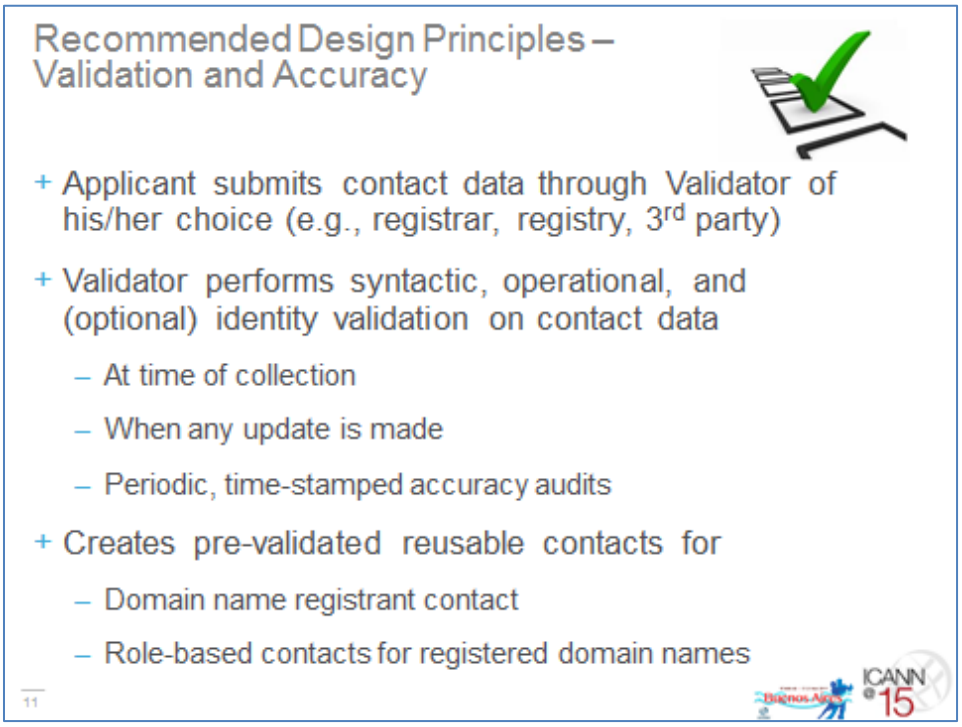
Sample RDS Record

Registry or Registrar Source	Registrant Source	Optional Role Based Contacts
Registration Status	Domain Name	Contact Name
DNSSEC Delegation	Name Server	Contact Role
Client Status	Registrant Name	Contact ID
Server Status	Registrant Type	Contact Organization
Registrar	Registrant Contact ID (issued by RDS-accredited Validator)	Contact Street
Reseller	Registrant Organization	Contact City
Registrar Jurisdiction	Registrant Company Identifier	Contact State/Province
Registry Jurisdiction	Registrant Email	Contact Postal Code
Registration Contract Language	Registrant Street	Contact Country
Creation Date	Registrant City	Contact Phone
Original Registration Date	Registrant State/Province	Contact Phone Ext
Registrar Registration Expiration Date	Registrant Postal Code	Contact Email
Updated Date	Registrant Country	Contact Fax
Registrar URL	Registrant Phone	Contact Fax Ext
Registrar IANA Number	Registrant Phone Ext	Contact SMS
Registrar Abuse Contact Email	Registrant Fax	
Registrar Abuse Contact Phone	Registrant Fax Ext	
URL of the Internic Complaint Site	Registrant SMS	

KEY: Bold Elements Always Public/Rest May Be Gated
Shaded Optional to Collect/Rest mandatory to Collect

14

The specific validation and verification requirements proposed by the EWG are summarized in the figure below, and listed on **Annex A** to this Request for Information.



Recommended Design Principles – Validation and Accuracy

+ Applicant submits contact data through Validator of his/her choice (e.g., registrar, registry, 3rd party)
+ Validator performs syntactic, operational, and (optional) identity validation on contact data
  – At time of collection
  – When any update is made
  – Periodic, time-stamped accuracy audits
+ Creates pre-validated reusable contacts for
  – Domain name registrant contact
  – Role-based contacts for registered domain names

11

Section 5.0 Instructions to Respondents

5.1 Definitions

"Respondent" means any person or firm receiving this RFI or submitting a response in response to this RFI.

"Syntactic Validation" refers to the assessment of data with the intent to ensure that they satisfy specified syntactic constraints, conform to specified data standards, and are transformed and formatted properly for their intended use. For example, if the data element is expected to be an email address is it formatted as an email address? In general, it is expected that syntactic validation checks would be entirely automated and could be executed in line with a registration process, follow up information reviews, and whenever registration data changes.

"Operational Validation" refers to the assessment of data for their intended use in their routine functions. Examples of operational validation include 1) checking that an email address or phone number can receive email or phone calls; 2) checking that a postal address can receive postal mail; 3) checking that the data entered are self-consistent, i.e. that all data are logically consistent with all other data. It is expected that many operational validation checks would be automated and some could be executed in line with a registration process.

"Identity validation" refers to the assessment that the data corresponds to the real world identity of the entity. It involves checking that a data item correctly represents the real world identity for the registrant. In general, identity validation checks are expected to require some manual intervention.

5.2 Timeline for Response

Responses are requested by close of business (UTC 23:59) on 7 March 2014 by email to: rfi-response@icann.org.

Annex A- Excerpts from the EWG Initial Report and Status Update Report

1. **Improving Accountability**

The proposed RDS takes a clean-slate approach, abandoning today's one-size-fits-all WHOIS in favor of purpose-driven access to validated data in hopes of improving privacy, accuracy and accountability.

As stated in its Initial Report, the EWG believes that a gated access paradigm could increase accountability for all parties involved in the disclosure and use of gTLD domain name registration data. First, the RDS would log all access to gTLD registration data, including anonymous access to public data elements, with restrictions to deter bulk harvesting. In addition, gated access to more sensitive data elements would only be available to requestors who applied for and were issued credentials for RDS query authentication. Finally, the RDS would audit both public and gated data access to minimize abuse and impose penalties and other remedies for inappropriate use. Different terms and conditions might be applied to different purposes. If requestors violate terms and conditions, penalties would apply.

DATA COLLECTION

Data must be collected before it can be selectively disclosed for permissible purposes. The following principles are suggested to guide collection at registration time:

No.	Principles for Data Collection
1.	To meet basic domain control needs, it should be mandatory for Registries and Registrars to collect and Registrants to provide the following data elements when a domain name is registered; this data would not necessarily all be sent to the RDS: a. Domain Name b. DNS Servers c. Registrant Name d. Registrant Type Indicates the kind of entity identified by Registrant Name: natural person, legal person, proxy service provider, trusted agent e. Registrant Contact ID A unique ID assigned to each Registrant Contact [Name+Address] during validation (refer to Section IV.b., for a more detailed definition of Contact ID and how it is created and used)

	f. Registrant Postal Address Includes the following data elements: Street, City, State/Province, Postal Code, Country (as applicable) g. Registrant Email Address Registrant Telephone Number Includes the following data elements: Number, Extension (when applicable)
2.	To avoid collecting more data than necessary, all other Registrant-supplied data used for at least one[1] permissible purpose should be optionally provided at the Registrant's discretion. Registries and Registrars must allow for this data to be collected and stored if the Registrant so chooses.
3.	To maximize Internet stability, the following mandatory data elements should be provided by Registries and Registrars to the RDS: a. Registration Status b. Client Status (Set by Registrar) c. Server Status (Set by Registry) d. Registrar e. Registrar Jurisdiction f. Registry Jurisdiction g. Registration Agreement Language h. Creation Date i. Registrar Expiry Date j. Updated Date k. Registrar URL l. Registrar IANA Number m. Registrar Abuse Contact Phone Number n. URL of Internic Complaint Site
4.	For TLD-specific data elements, the TLD operator should establish and publish a data collection policy (consistent with these over-arching principles) and be responsible for any validation of those TLD-specific data elements.
5.	Registries and Registrars may collect, store, or disclose additional data elements for internal use between the Registrar and Registrant, but never shared with the RDS.[2]

[1] The EWG is considering whether this should be one permissible purpose or two permissible purposes.

[2] Examples include the IP address used by the customer at the time of registration, a link to request generation of an EPP transfer key for a domain name, and payment data associated with the customer's account. Internal use data is not standardized by the RDS but rather privately defined by Registries and Registrars.

Principles identified by the EWG related to validation of data elements:

4.9	Validation and Accuracy	
	4.9.1	• To improve data quality, Registrant data should be validated syntactically (i.e., checked for correct format [per SAC58]) at the time of collection.
	4.9.2	• To improve usability, Registrant name/contact data should be validated operationally. (i.e., checked for reachability).
	4.9.3	• To reduce fraud ○ Registrants should be able to pre-validate by supplying a globally unique Registrant name/organization and associated contact prior to initial domain name registration. ○ Once pre-validated data has been checked for accuracy and uniqueness, an auth code (e.g., PIN) should be issued to that Registrant. No domain names should be registered with an identical[3] name/organization without supplying this auth code. ○ ICANN should enter into an appropriate contract with a third party provider to perform this pre-validation service and issue auth codes.
	4.9.4	• To promote consistency and uniformity and simplify maintenance, ○ Pre-validated data elements should be reusable – that is, applied to future registrations, with an option to over-ride these defaults on a per-domain name basis. ○ Any updates to pre-validated data elements could be automatically applied to all linked domain names.
	4.9.5	• To improve quality, Registrant name/contact data that is not pre-validated should still be validated in some way (e.g., implicitly via successful credit

[3] The EWG expects to explore this further.

	4.9.6 4.9.7 4.9.8 4.9.9 4.9.10	card payment with name/contact). • To preserve rapid activation while still promoting quality, delayed validation of Registrant name/contact should not prevent successful registration and DNS listing. However, such domain names could be flagged and suspended/deleted, if not validated within a defined period. • To enable successful Registrant name/contact validation globally, operational validation methods should not rely exclusively upon a single contact method (e.g., postal address). • To maintain the quality of data over time, validated data elements should be periodically re-validated – for example, whenever name/contact updates are made or domain names linked to a previously validated name/contact are transferred. • The system should record whether each data element was validated and when, even for data elements that are never disclosed. • To promote successful registration of domain names linked to high-quality name/contact data, Registrants must be educated about this process and associated policies.

4.10.	Standard Validation Service	

	4.10.1	• Use of a standard validation service is preferable because it:
		  ○ Reduces costs/burdens on Registrars/Registries.
		  ○ Enables more efficient licensing of validation databases such as UPS address cross-checking, yellow pages, corporate/company, government registries, electoral rolls, credit bureau records, etc.
		  ○ Standardizes the validation procedures as appropriate for a specific country/jurisdiction.
		  ○ Reduces the number of compliance inquiries on registries/registrars.
		• ICANN should enter into an appropriate contract with the third party provider of standard validation services in a manner that enables data accuracy compliance, auditing & availability.

	4.10.2	• ICANN should enter into an appropriate contract with the third party provider of standard validation services in a manner that enables data accuracy compliance, auditing & availability.

No.	Principles Related to Contact IDs
1.	In order to promote better accuracy, ease-of-use, and consistency of process, individuals, unique contact identifiers (Contact IDs) associated to specific sets of contact data should be issued to organizations, and other entities that publish "contact data" used for registry services. [4]
2.	Contact IDs are associated with discreet blocks of contact information necessary to play a role in a domain name registration.
3.	Contact IDs are issued by via accredited entities (e.g. registrars, registries, and third party validation providers) – referred to as Validators.
4.	In order be associated with a domain in any contact role, one must have an assigned Contact ID.
5.	Contact IDs can be assigned to multiple roles for one or many domains. E.g. registrant for one domain, technical and abuse contact with other domains.
6.	Contact IDs can be created as part of the domain registration process.
7.	A Contact ID can be validated at three different levels, syntactic, operational, and identity as per SAC 058.
8.	Validators can offer multiple levels of authentication for Contact Holders to utilize at their discretion, allowing for differing rigor to utilize or modify contact information for a particular Contact ID.
9.	Contact Holders may choose the level of authentication they desire to allow changes ranging from "none" to "high." [5]
10.	In order to preserve associations, a Contact ID can have a status of "inaccurate" and remain in the system.
11.	Active domains cannot have a mandatory contact with an "inaccurate" status without some sort of remediation, up to and including suspension.
12.	All data elements of contact data for a Contact ID must be validated at a syntactic level.
13.	Mandatory data elements for a contact identifier must be validated operationally prior to use of that Contact ID for a role related to a domain name.[6]
14.	A Contact Holder may seek higher levels of validation (e.g. fully validated at

[4] Such entities are "Contact Holders".
[5] For example, for a "high" authentication designation, multi-factor authentication may be necessary to access and change data associated with a Contact ID.
[6] More stringent option: The mandatory data elements for a Contact ID must be validated operationally and at least one primary contact data element be identity validated prior to use of that Contact ID for a role related to a domain name.

	the identity level) than minimum requirements dictate on a voluntary basis. [7]
15.	A minimum level of cross-field validation should be designated and routinely checked for all contacts.
16.	At a minimum, X[8] fields should be cross-field validated at the operational level meeting the applicable RAA.
17.	Revalidation of contact data should be carried out on a regular basis by the applicable validator. [9]
18.	Given the probable costs involved with identity validation, it is desirable to create a mechanism for economically disadvantaged applicants to receive identity validation.
19.	Validation Status of the Contact ID should be tracked and published as appropriate when accessing RDS information.[10]
20.	If a Contact Holder provides optional information for collection, it must be at least syntactically and operationally validated.
21.	For any given contact identifier, a Contact Holder may choose any particular Validator. [11]
22.	Oversight and accountability policies related to the management of the Contact IDs would need to be developed.[12]
23.	Changes to the contact data for a Contact ID must be made by the Contact Holder via the currently designated Validator. [13]

[7] This is akin to an EV CERT vs. a standard CERT in the CERT model. Rationale – an entity performing commerce or other sensitive transactions can increase consumer trust with higher levels of validation.

[8] The minimum number of fields to be validated is under discussion.

[9] For example, Syntactical validation should be carried out on at least an X interval, and operational validation should be carried out on at least a Y interval. If identity validation has been confirmed, then it should be rechecked on at least a Z interval. X, Y, and Z TBD.

[10] These values may include the following Statuses:

- Inaccurate
- Syntactically valid
- Operational valid
- Identity valid (verified)
- Unique

[11] Additional implementation processes would be needed to enable the contact holder to update that choice on his or her own prerogative following a designated confirmation process. For example, a corporation may choose to utilize just a single corporate registrar to manage all their contacts, ensuring a higher level of security, while a blogger may choose to use a Validator with a basic level of security. At some point in the future, the blogger could choose a different Validator and "transfer" management of their Contact ID and its associated contact information to that new Validator.

[12] For example, there would need to be some sort of controlled "transfer policy" and "transfer process" most likely similar to current domain name transfer policies and processes.

[13] Additional implementation procedures are needed here. For example, authenticated changes must be propagated to the authoritative data sources for such data, including all domain names utilizing the affected Contact ID. Depending upon the implementation model, this could include domain registries and registrars that store

24.	In order to combat impersonation, defamation, and abuse, a Contact Holder may designate that their contact data is unique and should not be used by other Contact Holder claimants. [14]
26.	If a Contact Holder requests a uniqueness designation, there should be a mechanism provided for other Validators to be able to compare a requested set of contact data against the Contact Holder's [see further analysis below].
27.	Contact Holders should be able to designate who may utilize their Contact IDs in association with domain name registrations. Potential levels of control include: • **Public** – anyone can designate the Contact ID as a contact for their domain • **Verified** – anyone can request the designation of a Contact ID as a contact for their domain, but the holder of the Contact ID must be contacted for approval prior to publishing the Contact ID as part of a domain registration.[15] • **Restricted** – for the highest security, the Contact ID can only be used by the Contact Holder who must be verified via some authentication mechanism. [16]
28.	A Contact Holder should be able to request that the use of their Contact ID in any domain registration (new or update) be tracked/reported and that they receive notification of such events, along with information about the entity making the request.

contact data associated with domain names.

[14] Conceptually this could be done at two levels:

- The full contact data set (i.e. the collective name, address, phone, e-mail) as associated with a Contact ID.
- Physically unique element "blobs" (e.g. individual address, phone, e-mail) that are part of a full contact record. Such "blobs" should represent a unique contact point that would in most cases be only usable to a specific person or entity.
- Some addresses may not be unique enough to qualify on their own, so in such cases, exception processes may be implemented.
- Unique data flag requests should be validated at the highest, "identity" level to gain such status.
- New requests to utilize flagged unique data elements without authorization should be blocked and potentially investigated for fraud.

[15] Implication is that some sort of approval/rejection process be created to facilitate such requests.

[16] Potential implementations methods include

- Restricting use of a Contact Id to a single registrar
- Multi-factor approval process to allow use at multiple registrars
- Implication of this is that some sort of status/usability restriction flag be published/provided to go along with the Contact ID itself.