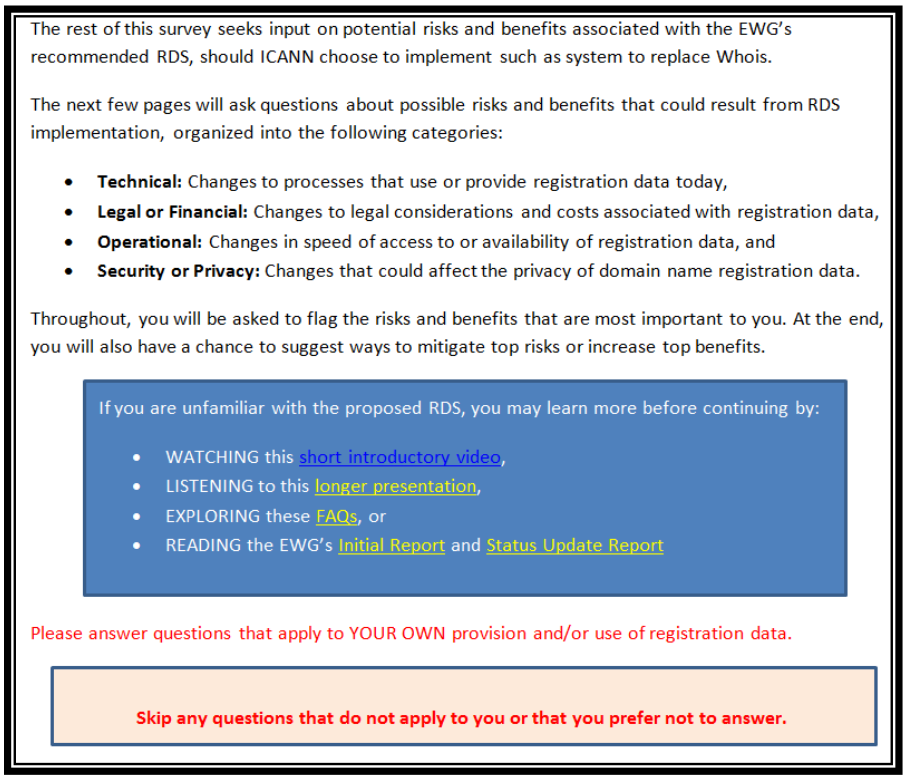
RDS Risk Survey – Result Summary

On March 14, the Expert Working Group on gTLD Directory Services (EWG) invited all parties that provide or use gTLD domain name registration data to participate in an RDS Risk Survey, including Registrants, Registrars, Registries, and the broad spectrum of individuals, businesses, and other organizations that consume Whois data today. This survey offered respondents a chance to tell the EWG about risks and benefits that the **Next Generation Registration Directory Service (RDS)** might have for them.

This document summarizes the RDS risks and benefits identified through this survey. The EWG used these survey responses to identify and reduce unanticipated and unnecessary risks when preparing its Final Report (published 6 June 2014). The EWG also recommended that these responses be used as input when conducting a future full risk assessment on the proposed RDS.

Survey Design

The introduction shown below set the stage by providing background for those unfamiliar with the RDS and organizing risks and benefits into 4 categories:



The rest of this survey seeks input on potential risks and benefits associated with the EWG's recommended RDS, should ICANN choose to implement such as system to replace Whois.

The next few pages will ask questions about possible risks and benefits that could result from RDS implementation, organized into the following categories:

- **Technical:** Changes to processes that use or provide registration data today,
- **Legal or Financial:** Changes to legal considerations and costs associated with registration data,
- **Operational:** Changes in speed of access to or availability of registration data, and
- **Security or Privacy:** Changes that could affect the privacy of domain name registration data.

Throughout, you will be asked to flag the risks and benefits that are most important to you. At the end, you will also have a chance to suggest ways to mitigate top risks or increase top benefits.

If you are unfamiliar with the proposed RDS, you may learn more before continuing by:

- WATCHING this short introductory video,
- LISTENING to this longer presentation,
- EXPLORING these FAQs, or
- READING the EWG's Initial Report and Status Update Report

Please answer questions that apply to YOUR OWN provision and/or use of registration data.

Skip any questions that do not apply to you or that you prefer not to answer.

For each category, respondents were shown example potential risks and benefits and invited to:

- *Select ALL Technical Risks that potentially impact YOU.*
- *Select TWO (2) risks that could have the biggest impact on you.*
- *Select TWO (2) risks most likely to occur.*
- *Select ANY newly-introduced RDS risk that is not already a known Whois risk.*

Respondents were also encouraged to add other potential risks and benefits. This summary of survey responses identifies the most commonly-cited risks and benefits, along with those write-in additions.

-- Published 28 July, 2014 --

RDS Risk Survey – Result Summary

Response Overview

This initial RDS Risk Survey was conducted in English, collecting 182 partial responses through June 12, 2014. Just over 100 respondents completed the entire survey.

All but one response was submitted prior to the EWG's Final Report publication. As such, these results offer feedback on the RDS as proposed in the EWG's Update Report (11 November 2013) and presented at ICANN48 in Buenos Aires. These results should not be viewed as feedback on the final RDS proposals detailed in the EWG's June 2014 report. Nonetheless, these responses helped the EWG understand what users and providers of Whois data believe to be potentially significant, impactful, and likely risks and benefits associated with *any* next-generation RDS.

Respondent Demographics

- Global representation, including North America (68%), Europe (35%), Asia (20%), Latin America (14%), Africa (12%), and Oceania (10%)[1]
- Evenly divided between those who USE and PROVIDE registration data:
    - 84% use registration data requested from Whois
    - 63% input data and 24% collect, store, or relay Whois data
    - Those USING data include Registrants (45-57%), individual Internet users (50%), business Internet users (50%), Internet technical staff (40%), Internet researchers (41%), OpSec investigators (36%), intellectual property owners (27%), other Investigators (14%), Law Enforcement agencies (5%), and roughly 20 others.
    - Those PROVIDING data include natural persons (65%), legal persons (59%), Registrars (14%), Registries (9%), Proxy Service Providers (5%), and third-parties (5%).

RDS Technical Risks

- Possible **negative technical impacts** most often cited (104 responses):
    1. I might no longer have anonymous public access to all registration data (69).
    2. Accreditation for access to gated data might be burdensome (65).
    3. My registration data access practices might need to change (62).
- Risks identified as the most impactful/most likely: 1 & 2 above.
- Beyond risks explicitly listed, additional technical risks identified:
    - New RDS might impact parties which provide historical and reverse Whois (8)
    - Automated access might not be available anymore (6)
    - Unable to get information about criminals, business partners, or applicants (3)
    - Turnaround time for obtaining data or registration might increase (2)
    - Privacy rights might be violated (2)
    - Single source of failure/ SAC061 technical risks (2)
    - Bulk information to law enforcement and spammers – two groups likely to abuse
    - Publicly searchable data will disappear
    - [Logins] I may use may have to be changed initially and ongoing due to turnover

[1] Note: Multiple responses allowed; total exceeds 100%

- Transfer/migration
- Cross-jurisdictional issue introduced
- No public scrutiny of registration data at registrars known to be tolerant of fake data
- Changes to registration data may require SSL certificates
- Breaks the delegated DNS model
- I lose logging visibility into who is accessing my personal data in some circumstances
- I lose ability to directly control or limit access to my information
- Development, QA, revision and update costs, with no revenue to offset them

General Note: Respondents identified all of these as technical risks, but many are actually covered as other kinds of risks, counted elsewhere in this survey.

RDS Technical Benefits

- Possible **positive technical impacts** most often cited (89 responses):
  1. Registration data that I access might be more accurate (58).
  2. Access to registration data might be more uniform and consistent (56).
  3. I might have better access to gated data that I really need (41).
- Benefits identified as the most impactful/most likely: 1 & 2 above
- Beyond benefits explicitly listed, additional technical benefits identified:
  - Improvement of data accuracy (through contact management and validation)(8)
  - I might have my data accessed by those who have legal entitlement to it, rather than published for all the world to see
  - I can more easily identify recidivist and serial cybersquatters before I file a lawsuit or UDRP complaint, thereby saving my clients money and resources
  - I will always have to provide port 43 Whois and it's not a big deal
  - Registration data accessed would likely be more applicable, helpful, and meaningful
  - Domain transfer between registrants will be easier (WHOIS data will stay the same, no parsing of Whois output needed anymore)
  - Negative impact due to large scale data mining reduced- Example: less spam

RDS Legal and Financial Risks

- Possible **negative legal and financial impacts** most often cited (102 responses):
  1. The amount of registration data that is freely available to all might decrease (68).
  2. My total cost for obtaining registration data might increase (66).
  3. RDS access logging or notification might compromise active investigations (51).
- Risk identified as the most impactful/most likely: 1 above
- Beyond risks explicitly listed, additional legal and financial risks identified:
  - Might make trademark infringers or spammers more difficult to track down. (3)
  - Time taken to access the data might be delayed (3)
  - Without public access to all data, I might make less value-added innovations.
  - Too many new TLDs lead to increased costs and lots of bad faith registrations.

- Lack of transparency of website owners (particularly for commercial sites with monetary transactions or personal data inputs) can be a risk to consumers.
- It may be difficult to confirm information about other domains a registrant has when confirming eligibility in the restricted domain.
- Failure would not be localized. one target for legal, DOS, control and other 'attacks'
- I might be required to provide non-existent information (e.g. real mailing address, yes there are people with no fixed abode who have domain names registered)
- The creation of a monopoly over Whois data will stifle innovation and centralize too much power over the Internet's "phone book" in one place.
- In some situations, that I am poking around is not a piece of data I would like shared, even with people who might otherwise be trusted.
- I want MY Whois data to be available for all interested parties as they are now
- Registries in the EU and in other places with data protection laws will not be able to export data to the RDS, greatly eroding its usefulness.
- Burden of costs and potential legal downside put on registrants, registrars, and registries with minimal benefit to impacted parties, maximal benefit to others.

RDS Legal and Financial Benefits

- Possible **positive legal and financial impacts** most often cited (68 responses):
  1. Improved quality of registration data might reduce costly inefficiencies (42).
  2. Contractual enforcement of data-related obligations might be more robust (35).
  3. I might find it easier to obtain lawful access to gated registration data (35).
- Benefits identified as the most impactful/most likely: 1 & 2 above
- Beyond benefits explicitly listed, additional legal and financial benefits identified:
  - My risk of having extensive amounts of personal data (including business data involving individuals) will decrease dramatically.
  - Easily make connections between domain owners and discover networks
  - I could send blame to ICANN/RDS provider for lack of transparency, and become less accountable.

RDS Operational Risks

- Possible **negative operational impacts** most often cited (87 responses):
  1. My access to registration data might be impeded by RDS failure (68).
  2. My access to gated data might be delayed by slow accreditation (66).
  3. My access to registration data might be slowed by RDS bottlenecks (65).
  4. RDS-returned registration data might not be synchronized with recent updates (56).
- Risks identified as the most impactful/most likely: 2 & 3 above
- Beyond risks explicitly listed, additional operational risks identified:
  - Relay and reveal response from accredited Privacy and Proxy services may be longer (7)
  - Our business would be at risk based on RDS policy decisions.
  - Gated access to the public does not allow consumers transparency to whom they're paying for services or when entering personal information

- Data breach
- May have increased difficulty/delay in dealing with network spam/attacks/issues coming from outside sources.
- Gated data for accreditation level may not meet actual requirement.
- Arbitrary rules will prevent valid access needs.
- I want ALL parties to have access to MY data using current established technology.
- Rogue sites that operate via network affiliate programs will be more easily shielded from Law Enforcement, service providers, & consumers who have been duped.
- Have to implement and maintain new process and system when status quo not broken.
- Additional time, revenue, and opportunity lost to increased initial contact by inexperienced IP counsel that will misuse or inappropriately leverage new system.

RDS Operational Benefits

- Possible **positive operational impacts** most often cited (61 responses):
  1. Relay and reveal responses from accredited Proxies may be shorter (40).
  2. I might have more reliable high-speed access to registration data (40).
  3. Real-time authenticated access to gated data may be faster than today (39).
  4. RDS response time might be more uniform and predictable than Whois (35).
- Benefits identified as the most impactful/most likely: 2 & 4 above.
- Beyond benefits explicitly listed, additional Operational benefits identified:
  - Aggregated RDS may better support features such as WhoWas and Reverse Whois (7)

RDS Security and Privacy Risks

- Possible **negative security and privacy impacts** most often cited (70 responses):
  1. My registration data might be more vulnerable to external attack (40).
  2. My registration data might be misused by the RDS operator (40).
  3. I might have to supply a verifiable identity to register a gTLD domain (24).
- Risks identified as the most impactful/most likely: 1 & 2 above
- Beyond risks explicitly listed, additional security and privacy risks identified:
  - "Individual Internet Users" are often rights owners and should have the ability to access relevant registration to investigate online infringement (5)
  - Concerned that individual users who should have access may be excluded
  - Supplying a valid phone number or email are essential for rights owners to investigate infringement
  - My registration data queries might be misused by the RDS operator
  - I might have to compromise rights that I have as both a legal person and a natural person by having to choose one or the other -- when my domain name registration and use clearly supports both. Therefore, I would be asked to relinquish rights under one category of rights, although I am legally entitled to the benefits of both.
  - Personal privacy risk that my data will become more available as a domain name administrator

- Loss of registrations because of the additional requirements; businesses in formation may not have business identifiers, etc. but still need a domain.
- External attackers will now have a big flashing red target.
- My personal identity may be forcibly associated with a domain owned and controlled by corporate entity, not by me personally
- Malicious individuals and organizations will take advantage of the ability to hide their information in the gated data, making it more difficult for security and compliance personnel to investigate them successfully.
- I can't register a domain anonymously
- Revealing my reasons for accessing data. They are legitimate, but they are my business, not ICANN's.
- Registration data might be less accessible by security, brand, and other private sector enforcement actors.
- My registration data will be more vulnerable to third parties, including those who handle private security functions for private firms and who will want more access to personal and sensitive information across multiple gTLDs.
- Possibility of being named in a lawsuit as a result of the availability of my name with the company
- Offering tiered access to law enforcement is a way of granting them extra access, and is a way around court orders and subpoenas. That's not the kind of opportunity or process ICANN should get involved in.
- Future registration data policy decisions could be made by a single entity.
- Third party access might contravene local law, data retention, or privacy and introduce legal exposure for customer without my knowledge.
- Third party access or stored data compromise could create wholesale tool for abusive use of my or my customer's data.
- New system could be new attack vector.

RDS Security and Privacy Benefits

- Possible **positive security and privacy impacts** most often cited (55 responses):
  1. My registration data might be better protected against misuse (37).
  2. My registration data might be more uniformly secured (31).
  3. I might publish a reusable Contact ID instead of my name (29).
  4. Less of my registration data might be public and anonymously available (27).
- Benefits identified as the most impactful/most likely: 2 & 3 above.
- Beyond benefits explicitly listed, additional security and privacy benefits identified:
  - Validation, Authentication and Authorization rules will be consistently applied and can be easily audited (7)
  - I would be more inclined to update my contact info to be accurate, as my stalker would not have access to it
  - Required to provide legal versus natural certification
  - Open access to legal entity better

RDS Risk Survey – Result Summary

Further Insights

Respondents offered 30 comments about **Unavoidable Risks**, elaborating on previously stated risks:

1. Access to registration data that is currently freely available will decrease.
2. Risks 5a, 5b, 9b (change in practices, reduced freely-available public access) are inherent in RDS.
3. Any entity that controls a singular central access point to retrieve registration data will always hold too much power over a public good.
4. The issue of unlimited access to the data even by those who have credentials is an issue the community needs to understand better. That the RDS is unlikely to check overbroad searches by state actors and third parties is a huge risk.
5. If the architecture fails, we will not have ready access to the information. Or the accreditation access takes too long.
6. Ability to obtain information in an efficient, timely fashion (to support clients pursuing rogue website investigations)
7. Ability to protect consumers from purchases and/or personal data entry on rogue websites (due to lack of transparency of site ownership)
8. Centralized storage and supply of Whois for all registrations in any sort of database (rather than from the registrars and registries) increases exposure to data breaches.
9. A system like this will be a magnet for those wishing to hack databases which could result in repeated slow service and outages.
10. I believe that it may be possible to get someone to provide some correct information at the time of registration but how will it be maintained?
11. Compliance with ICANN regulations are not the only reasons to provide WHOIS access. In practice the registry will always have to provide both port 43 and port 80 WHOIS access, increasing cost and risk.
12. RDS breaks a fundamental tenet of the Internet - devolution of power and control. It does so by introducing a whole bunch of new cross-jurisdictional issues in a technically deficient manner.
13. Ignores these problems: 1) How do I find a Whois server for a zone; 2) "private" domains which are open for "public" registration; 3) the installed base, existing tools and practices.
14. The new mechanism dictates much data is hidden. This will lead to an increased risk to the public as [problem] domains will not be actioned and escalated. Evidence would also be lost to law enforcement.
15. The current system requires a large amount of data to be provided. This data is vulnerable to capture on submission or in storage by those with dubious ethical standing as well as those with illegal intent.
16. Humans are involved - failure is built into the system.
17. Centralization of control over who can access domain name registration data, and the requirement for some sort of validation of the person or entity that accesses domain name registration data, creates an unavoidable risk of monopoly and reduced ability for law enforcement and security investigators to effectively identify abusive behavior on the Internet. These risks appear unavoidable [in either model].
18. An overall slowing of the domain registration process will be unavoidable if the registration data now needs to be validated.
19. The RDS proposes to extend gated access to law enforcement agencies of all/most countries. Therefore its very purpose is to expose individual registrants to investigation by foreign agencies, to whom they have no duty to obey or legitimate reason to subject themselves. Thus RDS is inherently flawed
20. Any mechanism for anonymous registrations will be abused. At least forcing the bad guys to register under a DBA and a PO Box provides a small barrier to entry to domain registration for criminal purposes.
21. Open access and impeding bulk replication of registration data both oppose the interests of domain registration profiteering, so it is unavoidable that any new RDS established by ICANN will "fix" those "problems" with the current Whois.
22. It is clear that the authors of the report are highly focused on protecting the privacy of a relatively small number of domain registrants with special privacy needs. However, legitimate cases of those sort are extremely few…The proposed changes will largely hinder the work of "do gooders", and will result in a domain ecosystem that's more prone to abuse, and more likely to be populated with inaccurate and non-useful data.

-- Published 28 July, 2014 --

23. Having big data is obviously a higher risk that cannot be avoided completely.
24. Any centralization of data poses the unavoidable risk of a single point of failure: hackers, cybercriminals, and badly-intentioned entities such as rogue governments or governments that abuse civil and human rights need look in only one place for private information.
25. Any restriction of public access to information about the identity of a domain's owner makes anti-malware and anti-spam research more difficult.
26. ICANN's dreadful track record in operations and compliance makes it completely implausible that this will work
27. My registration data will be located in another country, whose jurisdiction I don't trust.
28. It looks like the new RDS system will greatly improve the privacy of data registration therefore promoting free speech which in my opinion is the foundation and beauty of the Internet. My only concern in terms of unavoidable risks is in regard to the operators and employees as well as the people and organizations that will or could have unlimited and/or unregulated access to all registration data.
29. The centralized service is risky and unnecessary, and gets ICANN into sticky legal issues that can be avoided. Let's see some other potential solutions.
30. No matter the type or structure of kabuki theatre that might accompany where RDS originated or what it might thinly offer to anyone other than LEA or TM interests as benefit, this RDS will be perceived as a data source that the Governments will abuse.

13 respondents provided detailed responses and rationale about **Acceptable Risks**:

1. Risk is acceptable based on technical remedies that exist today (high performance computing, cloud based distribution and fail-over technology to increase availability, etc. (5)
2. As long as it is developed with generally accepted technical designed to ensure availability any security, concerns should be mitigated.
3. Non-commercial sites (that do not have ecommerce functionality or data entry requirements) pose less of a risk to consumers & those who strive to protect consumers (companies, law enforcement, etc.). Less transparency on these sites would be acceptable.
4. The ability to address varying privacy laws is an acceptable risk that potentially impacts business.
5. Risk of security breach of gated access data, is acceptable, as the risk is still less than it is now under the current public who is database.
6. The big data risk can be made acceptable by careful design and operational oversight. Lack of access to required information per gated access level can be ameliorated by careful analysis of stakeholder requirements.
7. ICANN would receive less 'Fees' as a result of implementing the RDS. The proposed RDS will reduce the registration volume that the market currently enjoys, due to the burdensome manner in which a customer must supply massive amounts of data before being able to make an initial purchase.

24 ways to **Reduce or Shift Risks** were suggested by respondents:

1. Steps taken to improve accuracy
2. RDS failure/bottleneck risks should be manageable through strong oversight of RDS operator.
3. Reverse Whois/WhoWas capabilities could be built into the RDS
4. Reduction in freely available data could be ameliorated through a rigorous analysis of data elements currently public and only suppressing public access to those for which the need for such suppression can be objectively established.
5. Designing a lightweight accreditation process leading to a persistent credential.
6. Identification of use of a name needs to be justified. The response should only be complaint based. If the request is valid then a response may be given.
7. Does the registrant receive a notice that the information has been requested and if so, identify the requesting party?

8. Top RDS risks can be avoided by only implementing the validator aspects into the current paradigm. If making all registration data conform to a specific format is desired, this could be accomplished by ICANN policy, rather than a new RDS.
9. Perhaps a way to delineate commercial from non-commercial sites to provide more transparency on commercial sites would reduce risk.
10. At least some of the risks may be reduced by using a federated approach with each registry storing their own information.
11. Re-think the entire scheme and collect minimal contact data. Apply standard principles of proportionality, privacy by design and privacy by default.
12. Require reasonable time limits for responses to contacts after which domains can be suspended pending response.
13. Store less data.
14. Whois access can and should remain anonymous and open to all Internet users.
15. Processing times for validation of registration data needs to be reduced as much as possible so that domain administrators can efficiently and effectively run their domains with minimal wait time due to validation procedures.
16. Allowing consumer choice in selecting a validation provider would be wise, so that providers are encouraged to keep costs and processing times down in order to be competitive.
17. Centralizing validation with a small group or forcing validation through a specific provider will decrease incentive to keep the process quick and cost effective.
18. Allow domain registration by anyone (not just people deemed in need of protection by some organization) completely anonymously, without providing any registration data. If there's almost no registration data, then there's no problem with public access to all of it.
19. Eliminate anonymity in registration.
20. Some risks can easily be softened by a phased approach to the implementation of RDS, for example by making any additional information requirements optional for a period while also making data available on the existing WHOIS infrastructure. This will mean that the RDS system can develop and any bugs/issues can easily be worked out without impacting the existing system, then once it's established and integration issues have had sufficient time to be worked on, registrars/registries can make the switch. I'd suggest a suitable period for additional data to be optional, and for the services to overlap to be ~3 years, this would allow for plenty of time to change systems and provide suitable education for customers.
21. Eliminate all "proxy" registration, enforce registration data accuracy, require registries to restrict bulk access, mandate open but rate-limited Whois access to all registration data, and prohibit sale of registration data in bulk by registries and registrars.
22. Eliminate the financial incentive for registrars or others to sell privacy registration services. Currently it's a cash cow, much as unlisted phone numbers were for the phone companies. Ensure that registrars make *nothing* from offering private or proxy-type registration services. Ensure that registrants who have a legitimate need for private or proxy-type registrants pay a fee sufficient to demonstrate that they genuinely need such a service, with all proceeds from such fees going to a public charity (thereby ensuring that ICANN also has no incentive to encourage private or proxy registrations)
23. Better consultation on required data versus gated access level.
24. In order to reduce the risk of abuse of access to private registration data, such access should be approved by legal documents signed by a judge or another legal authority.
25. To overcome Snowden/Kafka/Orwell perceptions of the wholesale abuse of this by overzealous interests, making all access and requests to the system fully 100% transparent to public viewing.
26. To overcome resistance to wholesale changes, figure out a method to increase benefits and reduce the downside to Registrants, Registrars, and Registries, such as Registry use of a centralized validation system.

13 respondents suggested ways in which **Risks were Good Tradeoffs for Benefits**:

1. Potential benefits depend on how it is implemented (2)

2. Any risks associated with decreased access to (currently free and public) data might be reduced if the community ensures greater data accuracy of any data that requires gated access. Reducing access without increased accuracy would be a major flaw in any proposed new system (2).
3. While an aggregated database could increase security risks, these can be ameliorated through proper design and oversight, and a ubiquitously available service that displays results in a consistent format could justify these risks.
4. Tiered access in exchange for better data (i.e., more complete and more accurate) might be one possible tradeoff.
5. The proposed RDS presents a number of benefits, which outweigh the risks. Easy access to accurate registrant data is critical to the enforcement of intellectual property rights online. An RDS system that improves access to and accuracy of this data would be extremely beneficial to intellectual property owners and their counsel in addressing IP infringement and other related abuses by domain name registrants and other internet users.
6. If validation costs and timelines can be controlled and kept to a minimum, the benefits of the proposed system could be a fair trade for the proposed benefits of the system. If costs are not controlled the costs will seriously outweigh the benefits.
7. Improving the quality of data in the Whois database is very important, and worthwhile. Linking registrants in a consistent way to their entire portfolio of domains is also very important and worthwhile, thereby ensuring that when an inaccuracy in point of contact data for one domain is identified and corrected, it gets corrected everywhere it exists.
8. Improved programmatic access (without arbitrary or ill-conceived rate limits, etc.) would also be tremendously helpful.
9. Uniform/reliable/useable access of the right data is a clear win since the risks can be minimized by careful design and consultation.

25 respondents offered **Further Comments** at the end of the survey, as follows.

1. The proposal lacks concrete features to improve the practical accuracy of data (the contact ability of registrants) significantly above the level that the baseline of 2013 RAA and (for new gTLDs) PICs. These need to be spelled out. Similarly, a richer database that provides enhanced services like historical data could help justify reduction of public access to this resource.
2. One benefit is to allow us to identify registrants that try to hide their identity so that they can continue with malicious activities and distributing malware.
3. The ability of users and 3rd party tools to use the current Whois system to access and save WHOIS information for historical purposes is critical. Any proposed RDS system must ensure this capability. This can happen either directly via the RDS itself, or indirectly by continuing to enabling 3rd party tools/clients to do so.
4. Giving monopolistic control of this public good to a singular entity results in a loss for the world with little benefit that could not be achieved via other, less-centralized, means.
5. Why are there so many new gTLD? This decision is disastrous for brand owners because it leads to increasing IP protection costs. Already now we are facing lots of bad faith registration although the sunrise periods for lots of new gTLD have not started even. As a smaller company you might not have the budget to register for all in order to avoid bad faith registrations. On the other hand legal appeal costs are high.
6. The fact to have a verified Whois is of the utmost importance due to the anonymity of the internet. We look for infringers and inaccurate data are no more acceptable.
7. I fully support the effort to make the WHOIS data more accurate. It would be a positive change IF a centralized, closed database does not make it more difficult to obtain information, slow down the process of obtaining information, have a cap on the amount of information that can be obtained, create long processes for companies to obtain accreditation to access info, or create issues of transparency for web users. Much of my concern lies with the cybersecurity community being able to effectively protect consumers from rogue websites that may gain an advantage from a closed database.

8. The proposed public vs. gated access for certain data elements is a good one. It would be helpful to see more details around acceptable disclosure purposes, evaluation of those applicants, ad how gated access users are held accountable, etc., in order to comment on that.
9. In general, any move to centralize data greatly increases the risks of overt and covert hacking, invisible and unaccountable government snooping, large-scale failure modes, and political interference. While some of the goals of RDS are valuable, they do not outweigh the entirely predictable risks. The greatest risks of RDS are the prospect of having to pay for access to public WHOIS information, and/or the loss of public access to basic network management information including IP address block assignment, physical location, and abuse mailboxes. Any proposal that does not protect free public access and continued availability of these information items should be swept off the table as quickly and definitively as possible.
10. I still not sure how we can ensure "accuracy" of the registration data, first-day data (on registration) is one thing , and another is "periodic check" which I think this is the most important. IMO, we may have to outsource this to "agency" in each locality (country or maybe town) to do the checking but this may leads to some question about accuracy and standard again.
11. The two groups of individuals that the average registry would like to prevent having bulk access to the Whois data are spammers and Law enforcement. Providing bulk information to either of these groups would irreparably harm the reputation of the registry. A centralized RDS system requires the registry to place its reputation in the hands of a third party.
12. There needs to be acceptance that not all parties have the same protectionism under local laws, that cross border requests for data may not follow due to external political issues. A vital resource in the fight against organized cybercrime will be lost with RDS.
13. As an individual registrant, I currently use a privacy/proxy function available from my registrar to shield my individual identity from casual, unnecessary access by the general public, which I find useful as a precaution against anonymous personal harassment. I'd like to see such privacy functions mandated to be regularly available whenever using any registrar, in order to ensure a fully-competitive registration market across all registrars, and not just a voluntary subset of registrars.
14. The top risk I am concerned about is cost for validation of my registration data, and authentication for me to access gated data. Also concerned about the processing times and general slowdown that these procedures will cause.
15. RDS is a great idea. This would help solve many problems if implemented properly. I look forward to having some input. However, this particular survey is not well constructed.
16. Frankly, this system seems to be as ill-considered as the currently available "WHOIS privacy" services. Using those merely hurts an organization's transparency and therefore their online reputation. Thank you for listening.
17. I see no benefits, but many risks with data misuse or theft. Ideally the need to provide registration data to the registrar would be eliminated - if there's no registration data, then there is no risk of its abuse or theft.
18. My concern is being able to deal with various sorts of network attacks/spam/intrusions/data flooding, etc. It is ABSOLUTELY essential that a valid contact exist, and that that contact will indeed deal with network issues reported to them. This means the contact must have both the authority and technical ability to ensure their domain is not the source of abuse. The current system, particularly those domains hiding behind proxies provides NO insurance that the registrar/proxy will (or can) address issues in a timely manner. If proxies are to be allowed, then it must be made ABSOLUTELY clear that whoever is listed in publicly accessible lookups/queries has the responsibility for the behavior of the domain they are shielding, including complete ability to shut down the domain in the event of significant network abuse.
19. The biggest risk is how access to "gated" information will be managed, such as if this will carry fees and how burdensome the accreditation process to get the access will be. If this is costly, or burdensome then it will seriously hinder basic business operations, contacting domain owners, research and numerous other areas of domain management and research.
20. I think this proposed process is a solution in search of a problem and fueled by specious straw man arguments by people driven by dogmatic political views.
21. I do not believe that careful consideration has been given to the privacy requirements of natural vs legal vs corporate/commercial entities. Individual/natural registrants need to be contactable in some way to

allow for remediation of problems that affect others, yet, must always be permitted the right of anonymity except in the case of appropriate legal request. In contrast, legal entities with only narrow restrictions (such as women's shelters, certain at-risk political organizations), MUST NOT have anonymity. It is absolutely inappropriate, especially with commercial enterprises, for them to operate anonymously and the data MUST be public/anonymous access. Secondly, there must be a process by which anonymity can be stripped from entities that are demonstrated to not quality for anonymity.

22. We suffer a lot from spammers and botnets using fake data to hide ownership of domains. Whois information can, and should, be clear and well-defined. It is not an undue hardship to obtain hosting services from other entities, but being clear on who is in charge of the DNS servers for a given domain is operationally useful.
23. In my opinion, privacy is far more important than public access to registration data.
24. Since there are no benefits, please stop doing what are you doing. If it works - do not fix it. Do not forget that a number of registrant DO WISH to have their Whois data accessible in the same way as they are now, and those who do not are free to use POB or registrar-offered privacy protection.
25. RDS is too much at once and a bad idea. It creates burden on those who least benefit, without real cost to those who most benefit.

Finally, approximately 5 of 182 respondents peppered most or all free-format text fields with answers that did not directly address questions, but instead stated the RDS was a bad idea or had no benefits.