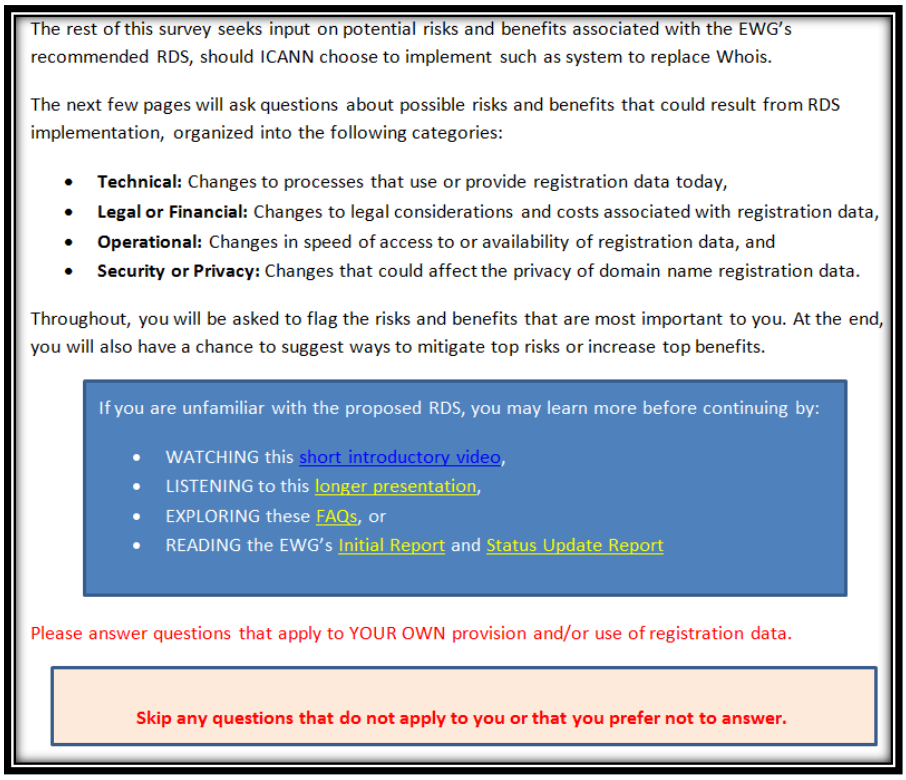
RDS 风险调查 — 结果摘要

3 月 14 日，gTLD 目录服务专家工作组 (EWG) 邀请提供或使用 gTLD 域名注册数据的所有相关方参加 RDS 风险调查，参与方包括注册人、注册服务商、注册管理机构以及当前使用 Whois 数据的个人、企业及其他组织。参与者可以通过本次调查告诉 EWG **下一代注册目录服务 (RDS)** 可能带给他们的风险和益处。

本文件对调查中得出的 RDS 风险和益处进行了总结。EWG 可以在编制最终报告（2014 年 6 月 6 日发布）时利用此次调查的结果识别并降低意料之外的和不必要的风险。此外，EWG 还建议在未来对 RDS 提案开展全面风险评估时，将调查结果作为建议考虑在内。

调查设计

下文中的简介部分为不熟悉 RDS 的调查对象提供了背景知识，并将风险和益处划分为四大类别：



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.

每一类别中都向调查对象提供有潜在风险和益处示例，并请调查对象：

- *选择所有会对自身产生潜在影响的技术风险。*
- *选择两 (2) 种对自身影响最大的风险。*
- *选择两 (2) 种最可能发生的风险。*
- *选择所有新引入的尚未成为已知 Whois 风险的 RDS 风险。*

该调查还鼓励调查对象添加其他潜在的风险和益处。本次调查结果摘要旨在说明最常提及的和补充填写的风险与益处。

RDS 风险调查 — 结果摘要

结果概述

此次调查是首次 RDS 风险调查，使用的语言为英语，截至 2014 年 6 月 12 日共收到 182 份部分回应。超过 100 名调查对象完成了全部调查。

除一份回应外，其余回应皆于 EWG 最终报告发布之前提交。调查结果针对 EWG 更新报告（2013 年 11 月 11 日）中提出的 RDS 提案提供反馈，该提案已在布宜诺斯艾利斯召开的 ICANN 第 48 届会议上公开展示。此次调查结果不能被视为最终 RDS 提案的反馈，该最终 RDS 提案在 2014 年 6 月的 EWG 报告中有详细介绍。尽管如此，调查结果仍可帮助 EWG 了解在 Whois 数据的用户和提供商眼中，可能存在的与*所有*下一代 RDS 有关的重要、影响深远或可能发生的风险和益处。

调查对象人口统计信息

- 调查对象来自全球，包括北美洲 (68%)、欧洲 (35%)、亚洲 (20%)、拉丁美洲 (14%)、非洲 (12%) 和大洋洲 (10%)[1]
- 注册数据用户和提供商在调查对象人数中各占一半比例：
    - 84% 的调查对象使用 Whois 提供的注册数据
    - 63% 的调查对象输入数据，24% 的调查对象收集、储存或中继 Whois 数据
    - 数据用户包括注册人 (45-57%)、互联网个人用户 (50%)、互联网企业用户 (50%)、互联网技术人员 (40%)、互联网研究员 (41%)、OpSec 调查员 (36%)、知识产权所有者 (27%)、其他调查员 (14%)、执法机构 (5%) 以及其他 20 类人群。
    - 数据提供方包括自然人 (65%)、法人 (59%)、注册服务商 (14%)、注册管理机构 (9%)、代理服务提供商 (5%) 和第三方 (5%)。

RDS 技术风险

- 最常提及的潜在**负面技术影响**（104 条回应）：
    1. 我可能将无法继续以匿名方式公开访问所有注册数据 (69)。
    2. 获取网关数据的访问认证可能会很繁琐 (65)。
    3. 我的注册数据访问操作可能需要改变 (62)。
- 确认为影响最大/最可能发生的风险是：以上第 1 项和第 2 项。
- 除已经明确列出的风险外，确认的其他技术风险包括：
    - 新 RDS 可能会对历史和逆向 Whois 提供方产生影响 (8)。
    - 自动访问功能或将无法继续使用 (6)。
    - 无法获取关于犯罪分子、企业合作伙伴或申请人的信息 (3)。
    - 获取数据或注册的周转时间可能会增加 (2)。
    - 隐私权可能会受到侵犯 (2)。
    - 故障来源单一/SAC061 技术风险 (2)。
    - 执法机构和垃圾邮件制造者（两个可能出现滥用行为的群组）获取大批量信息。
    - 可公开检索的数据将不复存在。
    - [登录] 因周转问题，我可能必须在首次登录和后续登录中更改信息。

[1] 注意：允许多次作答；比例总计超过 100%

- 转让/迁移。
- 引起跨辖区问题。
- 注册服务商处对注册数据的公众监督绝不容忍虚假数据的存在。
- 若要变更注册数据，或需获得 SSL 证书。
- 打破已授权的 DNS 模式。
- 在某些情况下，我无法查看我的个人数据访客的身份。
- 我丧失了直接控制或限制访问我的信息的能力。
- 没有收益可用于抵消因开发、QA、修订和更新而产生的成本。

总附注：调查对象将上述风险全部认定为技术风险，但实则其中很多风险都已经包括在本调查的其他类别的风险中。

RDS 技术益处

- 最常提及的潜在**积极技术影响**（89 条回应）：
  1. 我所访问的注册数据可能会更准确 (58)。
  2. 注册数据的访问可能会更具一致性 (56)。
  3. 我或许能够更加轻松地访问我真正需要的网关数据 (41)。
- 确认为影响最大/最可能产生的益处是：以上第 1 项和第 2 项。
- 除已经明确列出的益处外，确认的其他技术益处包括：
  - 数据准确度得以提升（通过联系人管理和验证实现）(8)。
  - 我的数据仅可由拥有合法权益的人士访问，而不是向全世界公开。
  - 在提起诉讼或 UDRP 投诉之前，我能更容易识别出惯犯和恶意抢注者，为我的客户节省金钱和资源。
  - 我必须每次都提供端口 43 Whois，但我不会感觉麻烦。
  - 所访问的注册数据或将更具适用性、实用性且更有意义。
  - 注册人之间的域名转让将更加简单（WHOIS 数据将保持原状，且无需再解析 Whois 输出）。
  - 因大规模数据挖掘而产生的负面影响将降低 – 例如：垃圾邮件数量减少。

RDS 法律与财务风险

- 最常提及的潜在**负面法律与财务影响**（102 条回应）：
  1. 所有人都可免费使用的注册数据的数量或将下降 (68)。
  2. 我获取注册数据的总成本或将增加 (66)。
  3. RDS 访问登录或通知或将危害到主动调查 (51)。
- 确认为影响最大/最可能发生的风险是：以上第 1 项。
- 除已经明确列出的风险，确认的其他法律与财务风险包括：
  - 商标侵权或垃圾邮件或将更难追踪。(3)
  - 访问数据所需的时间或将延迟 (3)。
  - 无法公开访问所有数据，我的增值创新或将减少。
  - 新 TLD 过多将导致成本增加和出现大量恶意注册。

- 网站所有者缺乏透明度（特别是开展货币交易或有个人数据输入的商业性网站），会对消费者构成风险。
- 在确认受限域名的资格时，要确认注册人持有的其他域名的信息或显困难。
- 不再定位故障。法律、DOS、控制和其他“攻击”共用一个目标。
- 或将要求我提供不存在的信息（如，真实的邮寄地址，确实存在没有固定住所的域名注册人）。
- Whois 数据垄断现象的形成将扼杀创造性，使得掌控互联网“电话簿”的权力过度集中在某一处。
- 在某些情形下，即使对方是值得信赖的人，我也不愿意与其分享我随意浏览的信息。
- 我想让我的 Whois 数据像现在这样对所有利益相关方可用。
- 欧盟及其他制定有数据保护法律的地区内的注册管理机构将无法向 RDS 导出数据，使得数据的可用性大打折扣。
- 注册人、注册服务商和注册管理机构所承担的成本压力和潜在法律劣势，使得利益相关方可获得的益处降到最低，并使其他方可获得的益处最大化。

RDS 法律与财务益处

- 最常提及的潜在**积极法律与财务影响**（68 条回应）：
  1. 注册数据质量的提升或将对成本低效起到缓解作用 (42)。
  2. 对与数据相关合同义务的履行或将更加有力 (35)。
  3. 获取网关注册数据的合法访问权限或将更加容易 (35)。
- 确认为影响最大/最可能产生的益处是：以上第 1 项和第 2 项。
- 除已经明确列出的益处外，确认的其他法律与财务益处包括：
  - 因持有大量个人数据（包括涉及个人的企业数据）而带来的风险将明显降低。
  - 各域名所有者之间可轻松地建立联系，查找网络也较容易。
  - 我可向 ICANN/RDS 提供商发送透明度缺乏的投诉，降低自身承担的责任。

RDS 运营风险

- 最常提及的潜在**负面运营影响**（87 条回应）：
  1. 我对注册数据的访问或将受到 RDS 故障的阻碍 (68)。
  2. 我对网关数据的访问或因认证缓慢而延迟 (66)。
  3. 我对注册数据的访问或因 RDS 瓶颈而放慢 (65)。
  4. RDS 返回的注册数据可能不会与新近更新的数据同步 (56)。
- 确认为影响最大/最可能发生的风险是：以上第 2 项和第 3 项。
- 除已经明确列出的风险外，确认的其他运营风险包括：
  - 从委任的隐私和代理服务方获取中继与披露回应或需更长时间 (7)。
  - RDS 政策决策可能会将我们的业务置于危险境地。
  - 公众网关访问不允许向付费服务供应商提供消费者透明信息，也不允许在输入个人信息时提供透明度。
  - 数据外泄。
  - 处理来自外部的网络垃圾邮件/攻击/问题的困难度或将增加，处理时间或将延长。

- 认证级别的网关数据或许不能满足实际要求。
- 随意性的规则会阻碍有效访问需求。
- 我想让所有相关方都能使用当前确定的技术访问我的数据。
- 通过网络附属程序运营的非法网站更难以被执法机构、已受骗的服务提供商和消费者识别。
- 必须在现状未被打破之前实施并维持新的流程和系统。
- 因 IP 顾问经验不足，误用或不恰当地使用新系统，造成初步联系增加，从而造成更多时间、收入和机会丧失。

RDS 运营益处

- 最常提及的潜在**积极运营影响**（61 条回应）：
  1. 从委任的代理服务方获取中继与披露回应所需的时间或更短 (40)。
  2. 我对注册数据的访问或将更加可靠和高速 (40)。
  3. 对网关数据的实时认证访问速度或将比目前更快 (39)。
  4. RDS 回应时间或将比 Whois 更具一致性和可预见性 (35)。
- 确认为影响最大/最可能产生的益处是：以上第 2 项和第 4 项。
- 除已经明确列出的益处外，确认的其他运营益处包括：
  - 集中式 RDS 或将更好地支持 WhoWas 和逆向 Whois 等功能 (7)。

RDS 安全与隐私风险

- 最常提及的潜在**负面安全与隐私影响**（70 条回应）：
  1. 我的注册数据或更易受到外部攻击 (40)。
  2. 我的注册数据或将被 RDS 运营商滥用 (40)。
  3. 我或需提供一个可验证的身份才能注册 gTLD 域名 (24)。
- 确认为影响最大/最可能发生的风险是：以上第 1 项和第 2 项。
- 除已经明确列出的风险外，确认的其他安全与隐私风险包括：
  - “互联网个人用户”通常都是权利持有者，他们应拥有访问相关注册的权限，以便调查网络侵权 (5)。
  - 担心本应该拥有访问权限的个人用户或将被排除在外。
  - 提供一个有效的电话号码或电子邮箱，对于权利持有者调查侵权行为至关重要。
  - 我的注册数据查询或将被 RDS 运营商滥用。
  - 我可能必须放弃作为法人和自然人本应拥有的部分权利，只能在二者之间选其一 – 尽管我的域名注册和使用明确支持我拥有这两类权利。因此，我将被要求放弃某一类别下的权利，即使我拥有合法的资格享受两种类别的权利带来的益处。
  - 在个人隐私风险上，作为域名管理员，我的数据可用性将更高。
  - 因条件的增加而造成注册减少；企业信息或未提供企业标识等，但对域名仍有需求。
  - 外部攻击者将拥有醒目的目标。
  - 我的个人身份或将被强制与由企业实体而非我个人所持有和控制的域名相关联。
  - 持有恶意的个人和机构会利用该功能，将他们的信息隐藏在网关数据中，让安全和合规人员难以成功地对其展开调查。

- 我无法以匿名方式注册一个域名。
- 披露我访问数据的原因。他们是合法的，但他们也是我的业务所在，不是 ICANN 的。
- 安全、品牌和其他私营领域执行人员访问注册数据的难度加大。
- 我的注册数据更易受到第三方的攻击，这些第三方包括为私营公司提供隐私安全服务的人员，以及想在多个 gTLD 中对个人及敏感信息拥有更多访问权限的人员。
- 可能因公司注册时列有我的名字而被提起诉讼。
- 向执法部门提供分级访问权限，不仅是授予他们更高访问权限的方式，也是规避法院指令和传审的办法。ICANN 不应该参与到这样的事件或程序中去。
- 未来的注册数据政策可能由单一实体做出决策。
- 第三方访问或将违反本地法律、数据保留或隐私，在我不知情的情况下给消费者带来法律风险。
- 第三方访问权限或储存数据泄漏，或将催生一种批量销售工具，导致我或我客户的数据被滥用。
- 新系统或将变身为新的攻击途径。

RDS 安全与隐私益处

- 最常提及的潜在**积极安全与隐私影响**（55 条回应）：
  1. 我的注册数据或将获得更好的滥用保护 (37)。
  2. 我的注册数据或将获得更加一致的保护 (31)。
  3. 我或可公布一个可重复使用的联系 ID，而无需公布我的姓名 (29)。
  4. 我的注册数据中能以匿名方式公开访问的内容会更少 (27)。
- 确认为影响最大/最可能产生的益处是：以上第 2 项和第 3 项。
- 除已经明确列出的益处外，确认的其他安全与隐私益处包括：
  - 验证、认证和授权规则的应用将更具一致性，也更容易审计 (7)。
  - 我将更愿意准确地更新我的联系信息，因为我的追踪者已无权访问我的联系信息。
  - 要求提供法律与自然认证。
  - 法律实体拥有更高的访问权限。

更多信息

调查对象提供了 30 条与**无法避免的风险**相关的意见，详细说明前文所述的风险：

1. 当前的注册数据免费访问将会减少。
2. 风险 5a、5b、9b（对实际做法的变更，免费公开访问减少）属于 RDS 的固有风险。
3. 任何控制某一中心访问点以检索注册数据的实体，对公共财产都拥有绝对的掌控权力。
4. 机构群体应更清楚地认识到持有认证的人士对数据的无限制访问这一问题。RDS 未必会检查国家机关和第三方过于宽泛的检索也是一大风险所在。
5. 如果该构架出现故障，我们便无法随时访问信息。或认证访问会花费很长时间。
6. 及时有效地获取信息的能力（为客户进行非法网站调查提供支持）。
7. 保护消费者不在非法网站上购买和/或不输入个人信息的能力（因网站所有者身份缺乏透明度）。
8. 在任何种类的数据库（而不是注册管理机构和注册服务商处）中集中储存和为所有注册提供 Whois 都会增加数据外泄的风险。
9. 此类系统将引诱那些不法分子入侵数据库，导致持续出现服务缓慢和运行中断。

10. 我相信在注册时让注册人提供正确的信息是可行的，但如何才能维持这一做法呢？
11. 符合 ICANN 规范并不是提供 WHOIS 访问权限的唯一原因。在实践中，注册管理机构始终都需要提供端口 43 和端口 80 WHOIS 访问权限，这不仅增加了成本，同时也提高了风险。
12. RDS　打破了互联网的一个基本原则 – 权力下放和实施管控。它通过一种存在技术缺陷的方式引入一整套全新的跨辖区问题，从而实现下放和管控。
13. 可忽略的问题包括：1)如何为某一区域找到一个 Whois 服务器；2) 面向“公众”注册开放的“私人”域名；3) 安装基础、现有工具和做法。
14. 新机制规定隐藏多数数据。由于 [问题] 域名未被执行或上报，这将对公众造成更大的风险。证据亦将丢失，对执法行动造成不便。
15. 当前系统需有大量数据供给。该类数据易被持不良动机及非法目的的人士在提交或储存中获取。
16. 存在人为因素 – 故障已内置到系统中。
17. 对域名注册数据访问权限的集中化控制，以及要求某人或某实体访问域名注册数据时提供某种验证，会造成不可避免的垄断风险，并削弱执法机构和安全调查员有效识别互联网上滥用行为的能力。[在任意一种模式下]，这些风险都无法避免。
18. 如果注册数据现在需要进行验证，那么域名注册流程速度的整体放慢将在所难免。
19. RDS 提议将网关访问权限扩展至所有/多数国家或地区执法机构。因此，该提议的目的正是将个人注册人公开显示给国外调查机构，注册人没有义务服从这些调查机构的命令，也不在法律上受制于后者。由此可见，RDS 存在固有缺陷。
20. 执行匿名注册的任何机制都将被滥用。至少强制要求不法分子在注册时提供公司经营业务所用的名称 (DBA) 和邮政信箱，可以为以犯罪为目的的域名注册行为设置一个小障碍。
21. 公开访问和阻碍注册数据的批量复制都能抵制通过注册域名获取利益的不正当行为，因此，任何一个由 CANN 创建的新 RDS 都将通过当前的 Whois“解决掉”这些“问题”。
22. 很明显，该报告的撰稿人将重点高度集中在保护相对而言一小部分需要特殊隐私保护的域名注册人的隐私上。然而，这一类合法案例的数量却寥寥无几…提议改变的内容将在很大程度上阻碍“行善人”的努力，导致域名生态系统更易遭受滥用，错误与无用数据或将更容易泛滥成灾。
23. 很显然，拥有海量数据是一个不能完全避免的高风险。
24. 任何数据的集中化都将构成不可避免的单一点故障风险：黑客、网络罪犯和恶意实体（如不良政府或滥用公民权和人权的政府）仅需访问一个地点即可获取私人信息。
25. 对域名持有人身份信息的公开访问做出的任何限制都将使得反恶意软件和反垃圾邮件研究变得更加困难。
26. ICANN 在运营和合规性方面糟糕的跟踪记录让人难以相信其可以发挥作用。
27. 我的注册数据将被存放在我对其管辖权不信任的其他国家/地区。
28. 看起来似乎新 RDS 系统将大大地提升数据注册的隐私，从而可以推广言论自由，在我看来，言论自由正是互联网的根基和魅力所在。对于不可避免的风险，我唯一担心的是运营商及其员工以及那些对所有注册数据均享有无限制和/或不受监管的访问权限的人和组织。
29. 集中式服务不仅存在风险，而且是没有必要的，并使 ICANN 深陷本可避免的法律纠纷之中。下面，让我们来看看其他潜在的解决办法。
30. 不论创建 RDS 时使用的歌舞伎剧院的类型或结构如何，也不论其除 LEA 和 TM 利益之外还能为每个人勉强提供的益处是什么，RDS 都将被视为会被政府滥用的数据源。

13 名调查对象提供了与**可被接受的风险**相关的详细回应和理由：

1. 如果风险可以使用当前技术（高性能运算、基于云的分布和提升可用性的失效备援技术等）予以修复，则该风险是可被接受的 (5)。
2. 只要开发中使用的是普遍接受的旨在确保可用性和安全性的技术，任何顾虑都能得到缓解。
3. 非商业性网站（不具备电子商务功能或没有数据输入需求的网站）给消费者和旨在保护消费者的机构（公司、执法机构等）构成的风险较低。这类网站拥有较低的透明度是可被接受的。
4. 应对各种隐私法律的能力将对企业构成潜在影响，但其是可被接受的风险。

5. 网关访问数据的安全漏洞风险可被接受，因为与当前公共数据库下的风险相比，该风险的威胁仍较低。
6. 通过仔细设计和运营监控，可将海量数据风险变为可接受的风险。对所需信息网关访问级别访问权限的缺失，可通过对利益主体需求的仔细分析得到改善。
7. RDS 的实施将造成 ICANN 可收取的“费用”缩水。RDS 提案将造成当前市场所具备的注册量下降，究其原因是，消费者在执行首次购买前，必须提交数量繁多的数据，其操作之冗长足以让人望而却步。

调查对象提出 24 种与**减轻或转移风险**有关的方法：

1. 采取措施提高准确度。
2. RDS 故障/瓶颈风险可通过对 RDS 运营商执行强有力的监管变得可控。
3. 可将逆向 Whois/WhoWas 性能内置到 RDS 中。
4. 免费可用数据的减少可通过对当前公开的数据元素展开精准的分析而得到缓解，仅针对可对其客观创建访问权限限制的访客限制其公开访问权限。
5. 设计一个简洁的认证流程，用于创建一个持续可用的凭证。
6. 须验证域名使用许可。仅能基于投诉进行回应。如果请求有效，则可给出回应。
7. 注册人是否收到一个信息请求通知，如果收到，是否可以识别出请求方的身份？
8. 通过仅在当前范例中实施验证程序，可规避首要的 RDS 风险。要让所有注册数据都符合特定的格式，可通过 ICANN 政策而不是新 RDS 来实现。
9. 或许以非商业性网站的角度来描述商业性网站，以提升后者的透明度可降低风险。
10. 至少可通过一种联合方式，即各注册管理机构负责储存各自的信息，来降低某些类别的风险。
11. 再三研究整个计划，尽可能少量地收集联系人数据。应用标准的比例性原则，通过设计和默认保护隐私。
12. 设置一个合理的联系回应时间限制，一旦超过该时间限制，将在等待回应期间暂停该域名。
13. 储存较少的数据。
14. Whois 访问可以且应该保持为匿名方式，并面向所有互联网用户开放。
15. 需尽量缩短注册数据验证的处理时间，让域名管理者能高效率地运行域名，而不会受到验证流程中等待时间的影响。
16. 允许消费者有权利选择验证提供商是明智之举，这样可鼓励提供商压缩成本、缩减处理时间，以此提高竞争力。
17. 将验证交由某一小型团队集中掌控，或强制通过某特定提供商进行验证，都将削弱保持流程快速运行和维持成本效益的积极性。
18. 允许任何人（不仅是某些机构认定为需要提供保护的人群）以完全匿名的方式注册域名，无需提供任何注册数据。如果注册数据极少，那么公开访问注册数据所带来的危害也就可以忽略了。
19. 废弃匿名注册方式。
20. 某些风险可通过分阶段实施 RDS 很轻松地得到缓解，例如，为某一时间段设置额外的可选信息要求，同时让数据也能在当前 WHOIS 基础构架上可用。这意味着在不对当前系统造成任何影响的情况下，可以开发 RDS 系统并纠正任何错误、解决任何问题，一旦创建成功且拥有充足的时间去解决集成问题，注册服务商/注册管理机构便可执行转换。我建议为额外数据设置一个合理的可选时间段，重叠服务期间大约为三年，以便有足够的时间更改系统和为消费者提供恰当的培训。
21. 取消所有“代理”注册，强制确保注册数据准确性，要求注册管理机构限制批量访问，强制要求以公开但有限的 Whois 访问方式访问所有注册数据，禁止注册管理机构和注册服务商批量出售注册数据。
22. 取消因注册服务商或其他方出售隐私注册服务而向其发放的财务奖励。目前，该服务是一个巨大财源，就像电话公司出售未编入册的电话号码一样。确保注册服务商从提供隐私或代理类注册服务中不能获得“任何利好”。确保有正当理由需要购买个人或代理类注册服务的注册人必须支付一笔费用，该笔费用的金额以足以证明其真正需求该服务为标准，所有此类收益全部捐献给公共慈善机构（由此可确保 ICANN 亦无意鼓励私人或代理注册行为）。
23. 针对网关访问级别对所需数据提供更好的咨询服务。

24. 为降低对私人注册数据的滥用访问风险，此类访问行为必须经由法官或其他合法当局签字的法律文件批准。
25. 为防止有人凭借过分热情对批量销售滥用注册数据产生斯诺登/卡夫卡/奥威尔式的看法，可让所有访问和系统请求对公众做到完全透明公开。
26. 为解决对批量销售变更的抵制行为，应寻找一种方法，为注册人、注册服务商和注册管理机构增加效益，降低不利因素，例如，让注册管理机构使用一种集中式的验证系统。

13 名调查对象提出的**风险与益处相权衡**的方法：

1. 是否存在潜在的益处取决于实施的方法 (2)。
2. 如果机构群体能保证需网关访问的所有数据获得更高的准确度，与（当前免费公开）数据的访问权限下降相关的风险都能得到缓解。访问权限下降但数据准确度却未提高，是任何一个拟议新系统的主要缺陷 (2)。
3. 虽然集中式数据库会增加安全风险，但此类风险可通过适当的设计和监管得到缓解，一种以统一格式展示结果且随处可用的服务可以减轻这类风险。
4. 使用分级访问取得质量更佳的数据（如，更加全面和准确）或将是一个可行的折衷办法。
5. RDS 提案所带来的一系列益处完胜其造成的风险。轻松访问准确的注册人数据对于维护网络知识产权而言无比重要。一个可以提升数据访问权限和数据准确度的 RDS 系统，对于知识产权所有者和其顾问在处理域名注册人和其他互联网用户的 IP 侵权及其他相关滥用行为中具有不可估量的价值。
6. 如果能将验证成本和时间线控制在最小范围内，拟议系统带来的益处将能抵消其带来的风险。如果成本得不到控制，由成本带来的弊端将超过其益处。
7. 提升 Whois 数据库内的数据质量极其重要且有意义。将注册人与其整个域名组以一种统一的方式相联系，同样也至关重要且意义重大，因此，应确保在发现并纠正某域名联系数据中的错误信息后，其余所有地方出现的此类错误信息也要得到纠正。
8. 改进的编程访问（无随意访问或考虑不周的访问等次数限制）同样具有很大的实用性。
9. 对适当数据的统一/可靠/实用访问是一大明显的优势，因为通过仔细设计和咨询可以将风险降到最低。

25 名调查对象在调查结束时提供了**更多意见**，内容如下：

1. 该提案缺乏可用于提升数据（注册人的联系信息）实际准确度的具体方法，其准确度要求远远高于 2013 RAA 和 PIC（适用于新 gTLD）基准的级别。这一点必须讲明。同样，提供增强型服务（如历史数据）且内容更加丰富的数据库，可有助于缓解对该资源公共访问的减少所带来的影响。
2. 其中一个益处就是让我们能识别出欲隐藏身份以继续开展恶意活动和散布恶意软件的注册人的身份。
3. 用户和第三方工具使用当前 Whois 系统以访问和保存 WHOIS 信息，以便进行历史记录的功能非常重要。任何拟议的 RDS 系统都必须确保具备此功能。该功能可直接通过 RDS 本身实现，或通过继续为第三方工具/客户提供此功能间接实现。
4. 此类公共财产的控制权由某单一实体垄断掌控将给全世界造成损失，使得通过其他集中化较低的方式可实现的益处变得愈加稀少。
5. 为什么会出现如此多的新 gTLD？这一决定对品牌所有人而言是一场灾难性损失，因为这将导致他们的 IP 保护成本随之递增。尽管许多新 gTLD 的日出期还未开始，但目前已经涌现出了数量繁多的恶意注册。对于小型公司而言，或许没有足够的预算用于通过注册所有域名来避免恶意注册。而另一方面又面临着高昂的法律上诉成本。
6. 由于互联网的匿名性质，持有经验证的 WHOIS 的重要性不言而喻。我们期待，侵权行为和错误数据将不再被接受。

7. 我绝对支持在进一步提高 WHOIS 数据准确度方面开展工作。如果集中化封闭式的数据库不会让信息的获取变得更加困难，不会降低信息获取过程的处理速度，不会限制可获取信息的数量，不会对获取认证以访问信息的公司造成冗长的认证获取流程，也不会为网络用户造成透明度问题，那么其可被视为一个积极的改变。我所关注的重点在于网络安全群体是否能有效地保护消费者不会在那些从封闭式数据库中牟取利益的非法网站遭受损失。
8. 相对于网关访问而言，某些数据元素的公开访问提案确实是一个良策。查看更多与可接受的披露目的、申请人评价及如何追究网关访问用户的责任等相关细节，将有助于对提案做出评论。
9. 总之，任何数据集中化措施都将大大增加公开和隐秘入侵、隐藏和无责任的政府窥探以及大规模故障模式和政治干预的风险。虽然 RDS 的某些目标极具价值，但却不足以抵消连带产生的所有可预见的风险。RDS 最大的风险是必须付费访问公共 WHOIS 信息，和/或无法公开访问基本的互联网管理信息，包括 IP 地址块分配、物理位置和滥用邮箱。任何不保护这些信息条目的免费公开访问和持续可用性的提案都应在第一时间内被完全废除，不予任何考虑。
10. 我不清楚我们应该如何确保注册数据的“准确度”，首日数据（注册首日）是其一，其二是“定期检查”，在我看来，后者才最为重要。我的观点是，我们应该将这方面的验证工作外包给各地点（国家或城市）的“代理商”，但这样又可能进一步导致一些与准确度和标准相关的问题。
11. 普通注册管理机构想要阻止两类人群批量访问 Whois 数据，即垃圾邮件发送者和执法机构。向这两类人群提供批量信息将对注册管理机构造成不可挽回的声誉损害。按照集中化 RDS 系统的要求，注册管理机构的声誉应置于第三方的掌控之中。
12. 我们应该接受这样一个事实，即并不是所有相关方都能享有本地法律规定的相同保护政策，且由于外部政治问题，跨境信息请求可能无法实现。RDS 或将失去对抗有组织网络犯罪的一个重要资源。
13. 作为个人注册人，当前我使用的是注册服务商提供的一个隐私/代理功能，用于保护我的个人身份不会被一般公众无意识或不必要地访问，我觉得该功能是一种具有实用性的匿名个人骚扰的预防措施。我的愿望是不论在与哪家注册服务商合作时，都能正常使用到该隐私功能，以确保能在所有注册服务商而非一小部分自愿注册服务商中建立起一个具有充分竞争性的注册市场。
14. 我所关注的首要风险是我的注册数据验证费用，以及我访问网关数据须提供的认证。另外，我还关心处理时间以及这些程序可能造成的总体速度减缓的问题。
15. RDS 是一计妙策。如果实施得当，它将能解决许多问题。我期待看到大家的建议。然而，本次调查的构建方式欠佳。
16. 实话说，该系统似乎被视为与当前可用的“WHOIS 隐私”服务一样欠妥。使用这样的系统只会对组织的透明度造成损害，进而损坏其名誉。谢谢大家。
17. 在我看来，该系统不仅毫无益处可言，而且会带来数据滥用和数据盗用的风险。理想的做法是消除向注册服务商提供注册数据的必要性 — 如果不存在注册数据，则不会出现对注册数据的滥用或盗用。
18. 我所关心的问题在于是否有能力去应对各种各样的网络攻击/垃圾邮件/入侵/数据泛滥等现象。存在有效联系人是绝对必要的，且该联系人确实会采取措施处理报告给他们的网络问题。这就意味着该联系人同时具备权限和技术能力去确保他们的域名不会成为滥用目标。当前的系统，特别是隐藏在代理背后的域名，不能保证注册服务商/代理商将（或能够）及时处理这些问题。如果代理商有权限采取此类措施，那么就必须澄清不论可公开访问的查询/询问列表中列出的相关方是谁，该相关方都必须对由其保护的域名产生的行为负责，包括在出现大量网络滥用时具备关闭域名的完全能力。
19. 最大的风险在于“网关”信息访问的管理方式，例如，如果访问会产生费用，那么获取访问权限所需的认证程序是否繁琐。如果获取访问权限成本高昂，或认证程序冗长，那么将会对基本业务运营、联系域名所有人、研究以及域名管理和研究的众多其他方面产生严重阻碍。
20. 我认为该流程提案是探究问题的一种解决办法，受教条主义政治观点影响的人士提出的似是而非的稻草人谬误对其起到了推动作用。
21. 我感觉并没有对自然/法律/企业/商业实体的隐私需求进行周密考虑。应通过某种方式与个人/自然注册人取得联系，以纠正会对他人造成影响的问题，且除非有正当的法律要求，否则都必须授予注册人匿名权。相对而言，具有更加细微的限制条件的法律实体（如妇女庇护所、某些面临危险的政治组织）则不允许享有匿名权。特别地，对于商业企业而言，要以匿名方式运营是绝对不可取的，此类机构的数据必须公开/可以匿名方式访问。其次，必须制定一个流程，用于剔除无资格享有匿名权的实体的匿名权。

22. 垃圾邮件和僵尸网络使用虚假数据隐藏域名所有人的身份，让我们饱受折磨。Whois 信息可以且应该清晰明了、定义明确。从其他实体处获取托管服务并不是过分之举，但是对于运营来说，明确了解谁在负责某一具体域名的 DNS 服务器会很有用。
23. 我的观点是，注册数据的隐私远远比公开访问重要。
24. 因为无利可图，请停止你的行为。如果有用 – 请勿纠正。请记住，确实有一部分注册人希望他们的 Whois 数据能保持现有的访问方式，对于不希望以现有方式访问 Whois 数据的注册人而言，则可自由使用 POB 或注册服务商提供的隐私保护。
25. RDS 有些过分，并非明智之策。它会对获利最低的人群造成负担，而获利最多的人群却不会付出任何真正代价。

最后一点，182 名调查对象中有大约 5 名人员在大部分或全部自由格式字段内没有填写与解决问题直接相关的答案，而是指出 RDS 并非明智之举，或毫无益处可言。