安全、稳定与弹性 (SSR2) 审核

执行摘要和概述

执行摘要

本报告是 SSR2 审核小组围绕调查结果和建议撰写的初步草案。SSR2 审核小组认为，除了有些项目需要持续反复调整之外，总体而言，凭借这份报告可以在征集公众反馈期间，收集到实用且关键的意见和建议，进而有助于形成最终报告。

特别值得一提的是，SSR2 审核小组非常希望能够征集到以下方面的反馈信息：

- 调查结果和建议；
- 应当由 ICANN 的哪个组成部分（例如，董事会、ICANN 组织，或 ICANN 社群）负责处理各项建议；
- 哪些衡量标准最适于衡量每项建议，同时还可以避免解决方案的过度设计；
- 应当如何设定每项建议的优先级；
- 审核小组在确定其建议之前，您认为还应当考虑其他哪些报告或资料（若要了解审核小组已查阅的资料，请参阅 SSR2 维基页面，[1]其中包括“背景资料”、“简报资料”以及“问答”环节）。

根据既定的社群审核流程，相关社群此后还将有机会在 SSR2 的最终报告中提供意见和建议。

概述

简介

[将在最终报告中补充。]

背景

[将在最终报告中补充。]

目标

按照《ICANN 组织章程》[2]（第 4.6(c) 节）中的规定：“董事会将围绕 ICANN 履行其承诺的状况开展定期审核，以此来提升内部和外部系统及流程中的运营稳定性、可靠性、弹性、安全性和全球互用性，这会与 ICANN 负责协调的互联网唯一标识符系统之间直接产生相互影响（即‘SSR 审核’）。”

具体要点：

ii. 负责 SSR 审核的审核小组（即“SSR 审核小组”）可能评估的议题包括以下内容：

A. 与协调互联网唯一标识符系统有关的物理和网络方面的安全、运营稳定性和弹性事项；

B. 是否符合互联网唯一标识符系统的适当安全应急规划框架；

[1] ICANN SSR2 审核小组维基页面，https://community.icann.org/display/SSR/SSR2+Review。

[2]《互联网名称与数字地址分配机构章程》，ICANN，于 2019 年 11 月 28 日修订，https://www.icann.org/resources/pages/governance/bylaws-en。

C. *对于 ICANN 协调的互联网唯一标识符系统的相应部分，是否维护了明确且全球互用的安全流程。*

iii. 此外，SSR 审核小组还将遵循 ICANN 的使命，评估 ICANN 组织成功实施其安全工作的程度，安全工作在处理 DNS 安全与稳定性的实际与潜在挑战及威胁方面的效果，以及安全工作在多大程度上足以充分而有效地应对 DNS 安全、稳定与弹性在未来所面临的挑战和威胁。

iv. SSR 审核小组也将评估此前 SSR 审核建议的实施程度，以及这些建议在实施后达到预期效果的程度。

v. 自上一轮 SSR 审核小组召开会议之日算起，执行 SSR 审核的频率不得低于每五年一次。

SSR2 建议 - 摘要

SSR2 审核小组已将所有的 SSR2 建议与《ICANN 2021-2025 财年战略规划》[3]及其目的和目标保持一致。本报告详细阐明了各项建议旨在实现的相关目标；SSR2 审核小组已从本报告中移除了没有与战略规划明确保持一致的所有建议。

SSR2 审核小组提出的所有建议均与 ICANN 组织的战略规划保持一致，因此应当被视为具有高优先级。

序号	建议	所有者	优先级
1	**完成所有相关 SSR1 建议的实施工作**		高
2	**SSR1 建议 9 - 信息安全管理系统和安全认证** 2.1. ICANN 组织应当制作一份路线图，以罗列其当前正在开展的符合行业规范的各项安全审核和认证活动，包括获取每项认证的里程碑日期以及需要不断改进的重点领域。 2.2. ICANN 组织应根据组织内各个职位的认证和培训需求，拟定计划、跟踪计划中各项认证和培训活动的完成率、阐明选择每项活动的理由，并记录各项认证如何融入 ICANN 组织的安全与风险管理战略。 2.3. ICANN 组织还应阐明其选择每个项目的原因，并展示每个项目如何融入其安全与风险管理战略。 2.4. ICANN 组织应实施信息安全管理系统，并接受第三方审核。 2.5. 为了充分发挥认证与审核机制的益处，ICANN 组织应依照行业安全标准接受第三方的审核与认证，并且应当根据普遍接受的国际标准（如 ITIL、ISO 27001、SSAE-18）来评估为其各项运营职能设置的认证方案。		高

[3]《ICANN 2021-2025 财年战略规划》，ICANN，最新更新日期：2019 年 3 月 29 日，https://www.icann.org/public-comments/strategic-plan-2018-12-20-en。

3	**SSR1 建议 12、15 和 16 - SSR 战略和框架、衡量标准及弱点披露** 3.1. ICANN 组织应秉持明确、公开的态度来处理各类安全问题（包括运营安全，例如，在需要的情况下，可制定暂缓方案并对信息进行匿名处理），促进所有签约方采用安全保障最佳实践。 3.2. ICANN 组织还应当将一些与 SSR 相关的最佳实践汇总到一份达成共识的文档中，并确立清晰、可衡量、可跟踪的目标，然后在合约、协议及谅解备忘录 (MOU) 中实施这些最佳实践。 3.3. ICANN 组织应实施协调性弱点披露报告流程。如果发现问题，例如，有签约方存在违规行为或者有人向 ICANN 组织报告发现了重大漏洞，则应当及时向受信任的相关方（例如，受指定问题影响或需要解决指定问题的相关方）传达有关 SSR 相关问题的弱点披露信息。 3.4. ICANN 组织应建立清晰明确的沟通计划以便向社群报告相关事宜，并且应当定期（至少每年一次）编制报告以便及时汇报相关问题，报告中应包含弱点披露流程的匿名衡量标准。这些公报应包含可靠的披露结果（由社群一致同意的流程所规定）以及匿名的衡量标准。		高
4	**SSR1 建议 20 和 22 - 新通用顶级域中 SSR 相关工作的预算透明度和预算规划** 4.1. 在可能（按合同规定）以及合理的范围内（即，预算行项目中描述的活动可超出 10% 的预算），ICANN 应当更加透明地公开其组织内部负责实施标识符系统安全、稳定与弹性 (IS-SSR) 框架和履行 SSR 相关职能（包括与新通用顶级域引入相关的职能）的部门的预算信息。		中
5	**SSR1 建议 27 - 风险管理** 5.1. ICANN 应对其风险管理框架进行战略性协调，从而使该框架成为集中式管理系统。 5.2. ICANN 组织应制定清晰明确的风险框架，并对该框架进行战略性调整以符合组织的要求和目标，该框架应阐明相关的成功衡量标准以及 ICANN 组织评估这些衡量标准的方式。 5.3. ICANN 应当向社群集中提供有关风险管理的信息。此外，ICANN 组织还应当定期更新此类信息以反映最新的威胁态势（至少应每年更新一次）。		高
6	**设立相应职位以全面负责安全战略和战术以及风险管理** 6.1. ICANN 组织应设立一个职位，以全面负责安全战略和战术以及风险管理，从而保障组织内部安全以及外部全球标识符系统的安全。 6.2. ICANN 组织应聘用满足相应条件的个人来担任此职位，并为其分配充足的特定预算以履行该职位的所有职责。		高

	6.3. 担任这个职位的人员应负责管理 ICANN 组织的安全职能，并在所有影响安全的相关领域中监管职员之间的互动往来。 6.4. 此外，担任该职位的人员还应当定期向 ICANN 董事会和社群提交报告。 6.5. 担任这个职位的人员应当作为一个探路者和问题解决者，负责制定战略并执行多方面的计划，从而推动相关工作取得显著改善。 6.6. 除此之外，担任该职位的人员还应当参与 ICANN 组织开展的所有关于安全事宜的合同协商工作（例如，硬件和软件供应链以及相关服务水平协议），并签字确认所有关于安全事宜的合同条款。		
7	**进一步制定安全风险管理框架** 7.1. ICANN 组织应制定清晰明确的安全风险管理框架，并确保该框架与组织需求和目标达成战略一致性。 7.2. ICANN 组织应阐明相关的成功衡量标准以及评估这些标准的方法。SSR2 审核小组已在针对 SSR1 建议 9 的补充反馈意见中阐述了该框架的基础（请参阅本报告前面部分中的“SSR1 建议 9 - 信息安全管理系统和安全认证”）。 7.3. ICANN 组织应当： 7.3.1. 采用并施行《ISO 31000 风险管理标准》，并通过适当的独立审核机制验证并认证这些标准的实施情况。[4]风险管理工作应当纳入业务连续性和灾难恢复计划与条款中。 7.3.2. 定期更新安全风险登记簿，并使用该登记簿对 ICANN 组织的各项活动进行优先排序和统筹指导。ICANN 组织应当报告有关所用方法及安全风险登记簿的更新。相关工作成果应当纳入业务连续性 (BC)/灾难恢复 (DR) 计划以及信息安全管理系统 (ISMS) 中。 7.3.3. 指定或任命专人负责安全风险管理工作，并向首席安全官（相关信息，请参阅“首席安全官职位”）汇报工作。		高
8	**根据 ISO 22301 制定业务连续性计划** 8.1. ICANN 组织应当根据《ISO 22301 业务连续性管理》[5]制定适用于其自身拥有或在其职权管理范围内的所有系统的业务连续性计划。 8.2. ICANN 应指明根据恢复全部功能的迫切程度，制定合理可行的业务连续性和灾难恢复时间表的重要性。 8.3. 对于 PTI 运营（即 IANA 职能，包括可促进 DNS 安全与稳定的所有相关系统以及根区管理），ICANN 组织应与根服务器系统咨询委员会 (RSSAC) 和根服务器运营商密切合作，共同制定实现服务连续性的共享方案。 8.4. ICANN 组织应发布与业务连续性计划和条款相关的材料（如摘要），以作证明。此外，还应聘用外部审核人员来核验制定的业务连续性计划的实施工作合规情况。		高

[4] 国际标准化组织，《ISO 31000 风险管理标准》，https://www.iso.org/iso-31000-risk-management.html。

[5]《ISO 22301:2019 安全与弹性 - 业务连续性管理体系 - 要求》，https://www.iso.org/standard/75106.html。

9	**确保灾难恢复计划合理可行且记录详实** 9.1. ICANN 组织应确保适用于 PTI 运营（IANA 职能）的灾难恢复 (DR) 计划涵盖了可促进 DNS 安全与稳定性的所有相关系统以及根区管理，且符合 ISO 27031《用于促进业务持续性的信息和通信技术配备指南》。ICANN 组织应当与 RSSAC 和根服务器运营商密切合作，共同制定该计划。 9.2. 此外，ICANN 组织还应制定适用于其自身拥有或在其职权管理范围内的所有系统的灾难恢复计划，该计划也应符合 ISO 27031《用于促进业务持续性的信息和通信技术配备指南》。 9.3. ICANN 组织应该在 ICANN 董事会采纳了以下这些建议的 12 个月内，制定一份灾难恢复计划，包括实施计划：至少要建立第三个灾难恢复站点（除洛杉矶和库尔佩珀之外），特别是在美国境外和北美地区外部建立相关站点。 9.4. ICANN 组织应对其所有灾难恢复计划和条款进行总结，并发布总结摘要。ICANN 组织应聘用外部审核人员来验证各项灾难恢复计划实施工作的合规情况。		高
10	**改善用于定义和衡量注册服务机构与注册管理机构合规程度的框架** 10.1. 制定一个绩效衡量标准框架，以指导评估注册服务机构和注册管理机构在 WHOIS 义务（包括信息错误）以及其他影响滥用、安全性和弹性的事项上所达到的合规程度，相关说明，请参阅 RDS/WHOIS2 审核和 CCT 审核。[6,7] 10.2. 为负责积极开展协定服务水平协议 (SLA) 衡量标准绩效管理检验/评估工作或委托他人开展该项工作的合规小组，分配特定的预算项目。 10.3. 将 SLA 续签条款从“自动续签”修改为“每四年续签一次”，后者包含一个审核条款（在审核期间，将根据绩效衡量标准考量注册服务机构和注册管理机构所达到的合规程度，若出现明显不合规的情况，将要求采取措施增强安全和弹性）。 10.4. 此外，ICANN 董事会应负责完成相应的快速政策制定流程 (EPDP)[8] 工作，并在相应报告发布后通过并实施 WHOIS 策略。		高
11	**带头促进滥用相关定义的发展演变并支持编制有关这些定义的报告** 11.1. 在与签约方签订的合同和实施规划中，ICANN 董事会应采取措施，以在最大程度上降低模糊性语言的使用，进而就滥用、SSR 和安全威胁确定普遍适用且一致同意的定义。		高

[6] ICANN RDS-WHOIS 审核小组，《注册目录服务 (RDS)-WHOIS2 审核：最终报告》，2019 年 9 月 3 日，https://www.icann.org/en/system/files/files/rds-whois2-review-03sep19-en.pdf。

[7] 《竞争、消费者信任和消费者选择：最终报告》，ICANN，2018 年 9 月 8 日，https://www.icann.org/en/system/files/files/cct-rt-final-08sep18-en.pdf。

[8] ICANN 通用名称支持组织，“供 ICANN 董事会审议的《gTLD 注册数据临时规范》GNSO 快速政策制定流程 (EPDP) 政策建议”，2019 年 5 月 1 日，https://www.icann.org/public-comments/epdp-recs-2019-03-04-en。

	11.2. ICANN 组织及董事会应毫不迟缓地根据经社群审核通过的现行滥用定义，履行与 SSR 相关的义务（包括 CCT 和 RDS/WHOIS2 审核建议）[9]。 11.3. 与此同时，ICANN 董事会应鼓励社群留意“DNS 滥用”一词定义（及应用）的发展演变，并采用新增术语“安全威胁”及其不断演变的定义，“安全威胁”这一术语在 ICANN《域名滥用活动报告》(DAAR) 项目和 GAC 公报（《北京公报》[10]规范 11[11]）中得到应用，且在国际惯例（例如《网络犯罪公约》及相关的“注释说明”[12]）中与 ICANN 组织的“DNS 滥用”定义结合使用。[13] 11.4. ICANN 董事会应委派安全与稳定咨询委员会 (SSAC) 和公共安全工作组 (PSWG) 与电子犯罪专家及滥用问题专家开展合作，将《网络犯罪公约》中规定的相关流程和定义纳入“DNS 滥用”这一术语的定义中，从而推动该术语定义的发展演变。		
12	**制定合法且可行的 WHOIS 数据访问机制** 12.1. ICANN 董事会应该为执法机构等相关方访问 WHOIS 数据，制定一个合法且可行的访问机制。 12.2. ICANN 董事会有责任确保 ICANN 组织及时完成《gTLD 注册数据临时规范》的实施工作。		高
13	**提高《域名滥用活动报告》的完整性和实用性** 13.1. ICANN 董事会和 ICANN 组织应与 ICANN 社群内部和外部所有致力于解决滥用问题的实体携手合作，提高 DAAR 的完整性和实用性，进而改善对域名滥用情况的评估和报告。 13.1.1. ICANN 组织应发布 DAAR 报告，以揭示通过 DAAR 方法识别出的域名滥用情况最为严重的注册服务机构和注册管理机构。		高

[9] CCT 报告中包含“DNS 滥用”及“DNS 安全性滥用”的定义，获得所需批准后，该报告第 8 页的脚注 11 引用了这两个定义，这两个定义包含在标题为“防止 DNS 滥用的保护措施（2016 年 6 月 18 日）”的 ICANN 员工文档中。注册滥用政策工作组 (RAP) 社群于 2010 年“就滥用一词的定义达成共识”，具体定义如下：“滥用是一种具有以下性质的行为：a) 导致实际和实质损害的行为，或可引发损害的实质行为；以及 b) 非法或不正当行为，或者以其他形式违背所规定合法目的的意图和企图（若此类目的已公开）的行为。”（获得所需批准后，CCT 最终报告第 88 页的脚注 287 引用了此定义）

[10] ICANN 政府咨询委员会，“GAC 建议：ICANN 第 46 届会议《北京公报》”，上次修改时间：2013 年 4 月 11 日，https://gac.icann.org/contentMigrated/icann46-beijing-communique。

[11] ICANN，《注册管理机构协议》，https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-09jan14-en.htm。

[12] 欧洲委员会，《网络犯罪公约》，ETS No. 185，第 7 页，2001 年 11 月 23 日，https://www.coe.int/en/web/cybercrime/the-budapest-convention。

[13] 请参阅注释 50

	13.1.2. ICANN 组织应通过 ICANN 开放数据倡议 (ODI) 公开 DAAR 的源数据，并在 ODI 数据资产库[14]中优先显示“*daar*”和“*daar-summarized*”等项目，以方便社群快速访问相关信息。 13.1.3. ICANN 组织发布的报告不仅应包含当前报告中的图形数据，还应包含机读格式的数据。 13.1.4. ICANN 组织应帮助董事会及所有选区、利益相关方团体和咨询委员会解读 DAAR 报告，包括帮助其识别有助于促进域名滥用预防和缓解的政策制定与咨询活动。		
14	**促进开展针对域名注册支付与安全威胁和滥用证据之间关系的严格定量分析** 14.1. ICANN 组织应收集、分析和发布价格数据，以进一步推动开展相关独立研究，并跟踪价格与滥用之间的关系。		高
15	**通过改善与注册服务机构和注册管理机构的合同条款来鼓励其缓解 DNS 滥用问题** 15.1. ICANN 组织应当在与签约方签署的协议（包括《注册管理机构协议》（基本版和个人版）和《注册服务机构认证协议》 (RAA)）中，围绕合同或基本协议的续订确立强制性的 SSR 要求。这些 SSR 合同要求应包含用于规定以下滥用阈值的条款：可自动触发合规问询的滥用率阈值（如注册总量的 3%）；可促使 ICANN 组织认定注册服务机构和注册管理机构违反其协议的较高阈值（如注册总量的 10%）。CCT 审核小组也建议使用此方法。[15] 15.2. ICANN 组织应新增一条合同条款，以支持在出现特定的滥用“行为模式或行径”后终止合同（请参阅 2013 年《注册服务机构认证协议》中的第 5.5.2.4 节“期限、终止和争议解决”）[16]。 15.3. 为支持相关方查阅上述合同变更，ICANN 组织应： 15.3.1. 确保相关方能出于合法目的，在履行合同义务并严格遵守合规机制的前提下访问注册数据。 15.3.2. 确立并执行统一的集中化域资料服务规定，以确保相关方能出于 SSR 查询目的而持续访问相关数据。 15.3.3. 吸引国家和地区顶级域 (ccTLD) 以及国家和地区名称支持组织 (ccNSO) 成员加入，与其开展合作，以促进解决 ccTLD 领域的 DNS 滥用问题和安全威胁。 15.3.4. ICANN 董事会、社群及 ICANN 组织应当与 ccNSO 携手合作，共同推动数据跟踪和报告工作、评估 ccTLD 领域的 DNS 滥用问题和安全威胁，并制定 ccNSO 计划以支持进一步缓解 ccTLD 领域的 DNS 滥用问题和安全威胁。		高

[14] 请访问：Https://www.icann.org/en/system/files/files/odi-data-asset-inventory-spreadsheet-11jun18-en.csv，由首席技术官办公室发布，网址为：https://www.icann.org/public-comments/odi-datasets-metadata-2018-06-11-en。
[15] 请参阅《竞争、消费者信任和消费者选择：最终报告》(https://www.icann.org/en/system/files/files/cct-rt-final-08sep18-en.pdf) 中的建议 14、15 和 16。
[16] 2013 年《注册服务机构认证协议》，ICANN，https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en。

	15.3.5. 立即要求签约方将 ICANN 组织地址空间列入其注册数据访问协议 (RDAP) 服务的白名单并落实此项工作；制定审查流程以指导签约方审查要列入其 RDAP 服务白名单从而授予速率不受限的访问权限的其他实体。 15.4. 从长远来看，ICANN 董事会应要求 GNSO 启动相应流程，以采用可显著缓解 DNS 滥用问题和安全威胁的新政策和协议（与签约方的协议），包括对 RDAP 和注册人信息进行更改、通过激励措施鼓励签约方积极解决滥用问题/安全威胁、建立绩效衡量标准框架，以及规定签约方和主要利益相关方所需开展的培训和认证活动。		
16	**通过制定价格激励措施来鼓励签约方积极解决滥用问题和安全威胁** 16.1. ICANN 组织可通过对合同做出以下更改，来激励签约方积极解决滥用问题和安全威胁： 16.1.1. 对于滥用域名比例（由商业提供商或 DAAR 确定）低于特定百分比（如 1%）的签约方，应向其提供费用减免优惠（例如，从当前总费用中减免一定数额，或提高当前每个域名的交易费用并为注册服务机构提供优惠）。 16.1.2. 对于由达到相应阈值且经过认证的注册人注册的每个域名，注册服务机构都应享有一定的费用减免优惠。 16.1.3. 如果签约方在注册管理机构服务评估政策 (RSEP) 文件中明确阐明其计划采用的 DNS 滥用缓解措施，并声明有注册管理机构 RSEP 已提前获得批准（即，批准注册管理机构级别的可扩展供应协议 (EPP) 授权由已认证的注册人管理的域名），则免除 RSEP 费用。 16.1.4. 对于被认定为存在滥用问题和安全威胁的域名，如果注册服务机构和注册管理机构能在注册后的合理时间内（例如，域名注册后的 30 天内）禁用这些域名，则向注册服务机构和注册管理机构退回相应的费用。 16.2. 由于所有相关方（ICANN 组织，签约方及其他主要利益相关方，例如，注册管理机构、注册服务机构、隐私/代理服务提供商、互联网服务提供商）都必须了解如何准确衡量、跟踪、检测并识别 DNS 滥用问题，ICANN 组织应采取制度化的手段，规定所有相关方开展相应的培训和认证活动，以帮助相关方了解由 DAAR 和其他关于常见滥用行为的报告 **[需补充相应引文]** 所指出的需改进领域，以及如何制定适当的缓解措施。培训应包含但不限于以下项目：自动跟踪投诉数量和投诉处理情况；发布关于投诉和投诉处理措施的季度/年度报告；分析。		高
17	**构建用于集中管理滥用报告的门户** 17.1. ICANN 组织应构建并维护用于集中管理 DNS 滥用投诉的门户，该门户可将每份滥用报告自动分发给相关方。此门户系统纯粹是流入型系统，系统上游只有摘要和元数据。所有 gTLD 相关方都必须使用此系统；应邀请 ccTLD 相关方加入此系统。对投诉所做的回应必须可公开搜索，且必须包含在年度报告（以完整形式包		高

	含或以引用形式包含）中。此外，应当向尚未加入系统的 ccTLD 相关方提供报告（例如，通过电子邮件）。		
18	**确保 ICANN 开展有效的合规性活动并客观审核合规性活动** 18.1. ICANN 组织应对其合规性活动进行外部审核，并在合规性活动上坚持高标准。 18.2. ICANN 董事会应授权合规部处理投诉，并要求合规部开展调查，同时针对协从与教唆系统性滥用行为（相关定义，请参阅 SLA）的相关方追究相应的合同责任。这项额外的授权允许逐步采取更加严格的法律措施以及其他适当可行的措施，ICANN 组织可在规定的时间范围内运用这些措施来纠正违规造成的任何失败。 18.3. 按照职责规定，ICANN 合规部应根据 SLA 来报告事件并执行措施；应采取明确、高效的流程；应向投诉人提供全面的信息；应评估满意度，并最大程度地公开信息。		高
19	**更新滥用命名的处理措施** 19.1. 在适当情况下，ICANN 组织应当与研究人员和利益相关方携手合作，进一步扩展当前进行的旨在调查常见误导性命名的活动。 19.2. 当误导性命名升级为滥用命名时，ICANN 组织应当将这种类型的滥用行为纳入 DAAR 报告中，并制定相应的策略和最佳缓解措施。 19.3. ICANN 组织应以适当形式发布门户中接收的滥用命名投诉数量，以允许独立第三方对此类域名的使用所带来的损害进行分析，并据此制定缓解和预防措施。 19.4. ICANN 组织应更新当前的《IDN 实施指南》**[需补充相应引文]**，以在其中增加有关含有商标、TLD 链及拼写错误（很难察觉）的域名部分。此外，ICANN 应通过合同，约定对 gTLD 强制执行《IDN 实施指南》，并建议相关方对 ccTLD 采取同样的措施。		高
20	**完成 DNS 回归测试的开发工作** 20.1. ICANN 组织应及时完成 DNS 回归测试套件的开发工作。[17] 20.2. ICANN 应确保实施并维护这项针对不同配置和软件版本进行功能测试的性能。		高
21	**实施 SAC063 和 SAC073 中的建议并制定用于指导密钥轮转的正式程序** 21.1. ICANN 组织应实施 SAC063 和 SAC073 中的建议，以确保密钥签名密钥 (KSK) 轮转流程的安全、稳定与弹性。		高

[17] “解析器试验床”，ICANN GitHub 库，https://github.com/icann/resolver-testbed。

	21.2. ICANN 组织应通过正式流程建模工具和建模语言[18]的支持，制定所需的正式流程，以规定后续密钥轮转的细节，包括决策点、例外路径、完整的控制流等等。对密钥轮转流程进行验证时，应发布编程过程（如程序、FSM）以进行公共评议，进而收集社群反馈意见。该流程的每个阶段都应具有凭借经验可验证的验收标准，只有达到这些标准，流程才能正常运行。该流程应接受反复评估，评估频率通常不应低于轮转本身的频率，以便能够及时使用所获得的经验教训，从而对流程进行调整。 21.3. ICANN 组织应组建一个由来自 ICANN 组织或社群的相关人员构成的利益相关方小组，该小组定期依照根区 KSK 轮转流程运行桌面演练。		
22	**制定适用于根服务器运营商和相关运营工作的基本安全措施** 22.1. ICANN 组织应当与 RSSAC 和其他关联的利益相关方密切合作，以确保 RSSAC037 中拟定的 RSS 治理模型包含适用于根服务器运营商和相关运营工作的基本安全最佳措施，进而在最大限度上降低与根服务器运营相关的 SSR 风险。这些最佳措施应涵盖变更管理、验证流程和完整性检查流程。 22.2. ICANN 组织还应制定相关的关键绩效指标 (KPI)，以评估相应最佳措施和要求的实施情况，并公开发布一个年度报告，以说明根服务器运营商 (RSO) 和其他相关方（包括 ICANN 组织）在多大程度上实现了这些 KPI。 22.3. ICANN 组织应记录 ICANN 管理的根服务器（IMRS，通常称为 L 根）所采取的强化策略，并鼓励其他 RSO 也如此效仿。 22.4. ICANN 组织应确保 IMRS 采用弱点披露流程（不一定要公开）及安全报告和情报，与相关研究人员沟通，并采纳 RSSAC 建议（如果适用）。		高
23	**加快实施新一代 RZMS** 23.1. ICANN 和 PTI 运营部门应加快实施有关变更请求验证和授权的新 RZMS 安全措施。 23.2. RZMS 策略在经过修订后，ICANN 组织应尽快发起公共评议。		高
24	**编制一份用于反映统一标识符系统运营状态的统计信息和衡量标准清单** 24.1. ICANN 组织应编制一份统计信息和衡量标准清单，以反映各类统一标识符信息的运营状态（如可用性和响应能力），包括根区相关服务的运营状态、IANA 注册管理机构的运营状态，以及在 ICANN 组织职权范围内的所有 gTLD 服务的运营状态。 24.2. ICANN 组织应在其网站的某一个页面上发布含有此类服务、相关数据集及衡量标准的目录，例如在开放数据平台下发布。		中

[18] 旨在改进关键的人员密集型流程之重要属性的迭代分析：选举安全示例，Leon J.Osterweil、Matt Bishop、Heather Conboy、Huong Phan、Borislava I.Simidchieva、George Avrunin、Lori A.Clarke、Sean Peisert，《ACM Transactions on Privacy and Security》(ACM 隐私及安全性事务，TOPS），卷 20，第 2 辑，2017 年 5 月，第 5 张幻灯片：1-31。(UM-CS-2016-012)

	24.3. ICANN 应当发布此类数据的年度和纵向摘要，并就这些摘要信息征求公众反馈意见，然后根据反馈意见改进未来的报告。 24.4. 对于上述每组 KPI，ICANN 组织都应根据上一年及纵向分析数据撰写摘要报告，就每份报告征求社群反馈意见并对社群反馈意见进行汇总，然后根据反馈意见来改进后续报告。		
25	**确保集中式域文件数据访问系统始终可用** 25.1. ICANN 社群和 ICANN 组织应采取措施，以确保有关请求人员在访问集中化域资料服务 (CZDS) 时，能像访问其他数据一样及时而顺利，不会遭受不必要的障碍。 25.2. ICANN 组织应实施 SSAC 97 中的四项建议：[19] *“建议 1：SSAC 建议 ICANN 董事会鼓励 ICANN 员工考虑调整 CZDS 系统，以解决订阅默认自动终止的问题，例如，通过允许订阅默认自动续订来解决此问题。为此，可以在系统中新增一个选项，以允许注册管理运行机构不对每个订阅者履行默认规定，从而强制要求选定的订阅者在当前订阅期结束后重新申请。CZDS 应继续支持注册管理运行机构随时明确终止存在问题的订阅者的访问权限。* *建议 2：SSAC 建议 ICANN 董事会鼓励 ICANN 员工采取措施，以确保在后续新通用顶级域轮次中，CZDS 订阅协议纳入因实施建议 1 而执行的变更。* *建议 3：SSAC 建议 ICANN 董事会鼓励 ICANN 员工采取有效方式，减少有关域文件访问的投诉，并及时解决投诉。* *建议 4：SSAC 建议 ICANN 董事会鼓励 ICANN 员工采取措施，以确保根据所有 gTLD 注册管理运行机构都能采用的明确且统一的标准，公开发布与域文件访问和基于 Web 的 WHOIS 查询相关的准确统计数据。应尽可能快地明确域文件访问 (ZFA) 衡量标准。*		高
26	**记录、改进和测试 EBERO 流程** 26.1. ICANN 组织应以公开的方式记录 ERERO 流程，包括决策点、相关操作和例外情况。记录文档应阐明每个决策、操作和例外情况的依赖条件。 26.2. 在条件允许的情况下，ICANN 组织应实现这些流程的自动化，并于每年测试这些流程。 26.3. ICANN 组织应根据之前通过与 ICANN 签约方协调而制定的测试计划，按照既定的时间间隔，以公开透明的方式开展 EBERO 冒		高

[19] ICANN 安全与稳定咨询委员会，“SAC097：关于集中化域资料服务 (CZDS) 和注册管理运行机构月度活动报告的 SSAC 公告”，2017 年 6 月 12 日，https://www.icann.org/en/system/files/files/sac-097-en.pdf。

	烟测试，确保测试所有的例外路径，并发布相关结果。ICANN 组织应允许 gTLD 数据托管代理直接将数据托管存储发送给 EBERO 提供商，进而改进流程。		
27	**更新 DPS 并就 DNSKEY 算法轮换构建共识** 27.1. PTI 运营部门应更新 DPS，以促进不同数字签名算法之间的轮换（包括从 RSA 数字签名算法转换到椭圆曲线数字签名算法 (ECDSA) 或未来的后量子算法），进而在不降低安全性的情况下增强 DNS 的弹性。 27.2. 鉴于根区 DNSKEY 算法轮换是一个非常复杂且敏感的过程，PTI 运营部门应与其他根区合作伙伴和全球范围内的社群合作，根据从 2018 年第一次根区 KSK 轮转汲取的经验教训，共同制定用于指导今后根区 DNSKEY 算法轮换的计划。		中
28	**编制衡量域名冲突频次报告并提出冲突解决方案** 28.1. ICANN 组织应总结各类域名冲突的性质和频次及所产生的问题，并编制相应的结果报告。ICANN 社群应在启动下一轮 gTLD 工作之前，实施相应的解决方案。 28.2. 为促进报告编制和解决冲突，ICANN 组织应启动并坚持完成独立的域名冲突研究，同时还应思考要采纳或实施哪些生成的建议。对 SSR2 审核小组而言，“独立研究”意味着 ICANN 组织应当确保 SSAC 域名冲突分析项目 (NCAP) 工作组调查结果和报告评估结果须由与 TLD 扩展没有任何财务利益关系的第三方进行审查。 28.3. ICANN 组织应支持社群报告域名冲突事件。此类报告应允许对敏感数据和安全威胁进行适当处理，且应该被纳入社群报告衡量标准。		中
29	**聚焦隐私和 SSR 问题衡量结果并根据这些结果改善相关政策** 29.1. ICANN 组织应监控并定期报告包括 DoT（基于 TLS 的 DNS）和 DoH（基于 HTTPS 的 DNS）在内的多项技术对隐私所产生的影响。 29.2. 因此，ICANN 组织与注册管理运行机构和注册服务机构达成的共识性政策和协议应包含相关条款，以反映合规情况，此外，由于需要维护/实施最低要求来规范注册数据（包括注册人、行政管理部门、技术部门的联系信息以及与域名相关的技术信息）的搜集、留存、托管、转让及显示事宜，还应同时确保 DNS 的完整性。 29.3. ICANN 组织应当： 29.3.1. 在合同合规部内部设立专门机构，以负责制定隐私要求和原则（例如，数据收集限制、数据分类、目的明细化原则，以及数据披露安全措施），并确保不断发展的 RDAP 框架满足执法机构的需求。		高

	29.3.2. 关注相关且不断变化的隐私法规（如 CCPA 和旨在保护个人身份信息 (PII) 的法规），并确保 ICANN 组织的策略和流程相互一致且符合相关法律法规所要求的隐私要求及个人身份信息保护。[20] 29.3.3. 制定并不断更新个人身份信息保护政策。应向参与处理个人身份信息的所有人员宣扬该政策。应当实施能有效保护 PII 的合理技术措施和组织管理措施。 29.3.4. 定期对注册服务机构隐私政策履行情况进行审核，以至少确保注册服务机构制定了用于处理侵犯隐私行为的流程。 29.4. ICANN 组织的数据保护主管 (DPO) 还应负责管理外部 DNS PII。DPO 应向相关管理人员和利益相关方提供有关职责划分和适用流程的指导，并关注和报告相关技术进展。		
30	**持续关注有关 SSR 问题的学术研究并使用相关信息促进政策讨论** 30.1. ICANN 组织应跟踪同行评审研究社群中的进展，主要应当关注网络和安全研究会议，其中至少包括 ACM CCS、ACM Internet Measurement Conference（ACM 互联网衡量标准会议）、Usenix Security（Usenix 安全）、CCR、SIGCOMM、IEEE S&P，以及运营安全会议（APWG、M3AAWG 和 FIRST），并发布一份概述报告以总结与 ICANN 组织或签约方行为有关的出版物的结论，供 ICANN 社群参阅。 30.1.1. 此类报告中应提供可行的措施建议（包括针对与注册管理机构和注册服务机构签署的合同进行更改），这些措施应有助于缓解、预防或纠正同行评审文献中指出的消费者和基础架构所遭受的 SSR 损害。 30.1.2. 此外，这些报告中还应提供有关开展其他研究以确认同行评审成果的建议，其中应当介绍为了开展推荐的其他研究所需的数据，以及 ICANN 提供相关数据访问权限的代理方法，例如 CZDS。		中
31	**明确 DoH 对 SSR 的影响** 31.1. ICANN 组织应授权开展独立调查，以研究 DoH（基于 HTTP 的 DNS）部署趋势对 SSR 及 IANA 今后在互联网生态系统中的作用所产生的影响。该项调查旨在确保所有利益相关方都能了解 DoH 技术发展对 SSR 所产生的影响，以及他们各自所具有的足以影响未来发展的其他选择（或者缺乏其他选择）。		高

[20] 审核小组了解到 ICANN 组织发布了关于政府合作方案的章程 https://www.icann.org/en/system/files/files/proposed-org-engagement-govt-standards-charter-25feb19-en.pdf 和相关立法报告（立法跟踪）https://www.icann.org/legislative-report-2019。但是，我们希望聚焦于更为具体的隐私和数据保护问题。

适用于未来 SSR 审核小组的指导意见 - 要点

为了简化未来 SSR 审核小组开展的评估工作，SSR2 审核小组将努力制定符合 SMART 标准的建议，即：尽量制定“具体”、“可衡量”、“可分配”、“相关”且“可跟踪”的建议。SSR2 审核小组认为，若能制定更加清晰的以行动为导向的建议，将有助于简化下一轮 SSR 审核中的实施、跟踪和评估工作。关于 SSR2 审核小组为履行其职责而采用的流程和方法的补充信息，已包含在“附录 C：流程和方法”中。
