第二轮安全、稳定和弹性 (SSR2) 审核小组最终报告——执行摘要与建议

摘自 SSR2 审核小组最终报告

2021 年 1 月 22 日

目录

A. 执行摘要

根据互联网名称与数字地址分配机构 (ICANN) 章程（第 4.6 (c) 节）的规定：

“*董事会应指示就 ICANN 对以下义务的履行情况展开审核（SSR 审核）：增强内外部系统和流程的运营稳定性、可靠性、弹性、安全性和全球互用性，这些系统和流程与 ICANN 负责协调的互联网唯一标识符系统之间存在着直接的相互影响关系。*”[1]

这些 SSR 审核是完成 ICANN 组织“运作上秉承公开和透明的原则实现最大程度的可行性，并遵守那些为确保公正性而设计的程序”使命 [2]的重要组成部分。这是开展的第二轮 SSR 审核，并且根据章程规定，审核报告中包含了对 ICANN 组织处理第一轮 SSR 审核建议的综述以及供 ICANN 组织审议的新建议。

SSR2 审核小组提出了 24 组建议，包括 63 项具体建议，从对 ICANN 组织针对 SSR1 建议的回复的评估开始。我们采用这种将建议进行细分的方法是为了解决 SSR1 建议中缺乏明确性的问题。然后再将这些建议分门别类，以提供对以下几方面情况的分析：ICANN 组织内部运营、ICANN 组织合作（特别是对合同和投诉的处理），以及 ICANN 组织如何采取措施来改善自身的 SSR 工作并帮助其他人了解如何改善他们的 SSR 工作。整个文档中的各项建议往往会相互影响，并且各项建议之间存在相互依赖关系。ICANN 组织和董事会在制定实施规划时应考虑到这一点。每项建议都获得了审核小组全体成员的一致同意。

为支持未来 SSR 审核小组提高评估效率，SSR2 审核小组努力制定符合 SMART 标准（*具体*、*可衡量*、*可分配*、*相关且可跟踪*）的建议。在许多情况下，使每项建议都完全符合 SMART 标准所需的详细信息，包括指定适当的时间表，都离不开实施团队的审慎思考和行动，因此应纳入最终实施计划中。审核小组还就如何处理未来审核轮次提出了几项建议供审议，同时认识到这些建议所涉及的问题不属于 SSR 审查本身的直接使命范围。“附录 C：流程和方法”中提供了关于 SSR2 审核小组在履行自己的使命时所遵循的流程和采用的方法的更多信息。

1. 背景

如 A.2 部分“SSR 审核目标”中所述，《ICANN 章程》要求定期评估域名系统 (DNS) 的安全、稳定与弹性。2012 年 9 月 13 日，ICANN 董事会正式收到第一轮 SSR 审核报告。五年后，于 2017 年 3 月 2 日举行的 SSR2 审核小组启动会议开始了第二轮审核工作。然而，SSR2 审核小组自成立以来遇到了一些挑战，致使审核持续时间远远超出了所有人的预期。SSR2 审核小组定期举行会议，直到 2017 年 10 月 ICANN 董事会暂停了该审核小组的活动。[3] 2018 年 6 月 19 日，小组成员重组后再次召开会议。[4]

[1] ICANN，“互联网名称与数字地址分配机构章程：第 4.6 (c) 节：特定审核：安全、稳定与弹性审核”，2019 年 11 月 28 日修订，https://www . ICANN . org/resources/pages/governance/negotiation-en/# article 4。

[2]《ICANN 章程》，第 3.1 节：https://www.icann.org/resources/pages/governance/bylaws-en/。

[3] ICANN 董事会主席史蒂夫 • 克罗克 (Stephen D. Crocker) 博士致 SSR2 审核小组的信函，2017 年 10 月 28 日，https://www.icann.org/en/system/files/correspondence/crocker-to-ssr2-28oct17-en.pdf。

[4] ICANN 博客“第二轮 DNS 安全、稳定和弹性审核 (SSR2) 重新启动”，2018 年 6 月 7 日，https://www.icann.org/news/announcement-2-2018-06-07-en。

在审核流程延长期间，全球唯一标识符生态系统的格局继续不断变化。新型冠状病毒肺炎 (COVID-19) 疫情导致国际商务和差旅中断，给 SSR2 审核流程带来了更多延误，尽管如此，SSR2 审核小组仍然完成了这一轮审核。在审核流程的最后一年，审核小组选择不重新开始评估其最初的建议，而是保留以前的基本建议。审核小组认为，这些建议在很大程度上仍然与 ICANN 组织息息相关，并可为全球 DNS 的安全、稳定与弹性提供有力支持。

2. SSR 审核目标

《ICANN 章程》第 4.6 (c) 节规定："*董事会应指示就 ICANN 对以下义务的履行情况展开审核（SSR 审核）：增强内外部系统和流程的运营稳定性、可靠性、弹性、安全性和全球互用性，这些系统和流程与 ICANN 负责协调的互联网唯一标识符系统之间存在着直接的相互影响关系。*"[5]

具体而言，它规定了：

"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：

1. *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；*
2. *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；*
3. *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。"

3. 其他审核小组和咨询委员会的影响

根据《ICANN 章程》的规定，ICANN 组织必须与多个审核小组和咨询委员会 (AC) 合作。虽然这些小组和委员会都有各自具体的职责，但他们提出的建议可能而且确实与其他审核小组和委员会的工作领域重叠。SSR2 审核小组评估了其他审核小组和 AC 的建议，以确定他们发布的建议会对 ICANN 组织以及全球 DNS 的安全、稳定与弹性 (SSR) 造成怎样的影响。在某些情况下，SSR2 审核小组发现有必要纳入并借鉴这些建议，为 ICANN 组织制定与 SSR 相关的必要指南（详情请参阅第 E.1 节：未实现的新通用顶级域项目保护措施，以及第 E.3 节：PDP 替代方案）。SSR2 审核小组认为，建议中的这些重叠之处是对相应问题重要性的默示确证，并且还认为，在 SSR2 审核小组的建议与其他团体的建议之间达成共识，是对提出这些建议的必要性的实证支持。SSR2 建议旨在对其他审核小组的建议进行补充。

[5] 《ICANN 章程》第 4.6 (c) 节，https://www.icann.org/resources/pages/governance/bylaws-en。

B. SSR2 建议

每项建议都获得了 SSR2 审核小组全体成员的一致同意。

1. 汇总表

序号	建议	所有者	优先级
SSR2 建议 1：进一步审核 SSR1 建议			
1.1	ICANN 董事会和 ICANN 组织应进一步全面审核 SSR1 建议，并执行一项新计划来完成 SSR1 建议的实施（请参阅附录 D：与 SSR1 建议相关的审核结果）。	ICANN 董事会和 ICANN 组织	低
SSR2 建议 2：设立相应的高级管理层职位，全面负责安全战略和战术以及风险管理			
2.1	ICANN 组织应在组织内部的高级管理层设立一个首席安全官 (CSO) 或首席信息安全官 (CISO) 职位，同时聘请适当的合格人员担任此职务并分配足够的具体预算助其履行自身职责。	ICANN 组织	中 - 高
2.2	ICANN 组织应在这个职位的职责说明中指出，此职务负责管理 ICANN 组织的安全职能，并监督所有可能会影响安全性的相关领域的员工互动。这一职务应负责定期向 ICANN 董事会和社群提供关于 ICANN 组织内所有 SSR 相关活动的报告。现有的安全职能部门应进行重组并调整组织架构，均向此新职务负责人汇报。	ICANN 组织	中 - 高
2.3	ICANN 组织应在这个职位的职责说明中指出，此职位负责制定安全战略和战术以及风险管理。这些职责领域包括：领导并战略性地协调组织内部安全领域的集中风险评估、业务连续性 (BC) 和灾难恢复 (DR) 计划（另请参阅 SSR2 建议 7：改进业务连续性和灾难恢复流程和程序），包括 ICANN 管理的根服务器（IMRS，也称为 L 根），并与外部全球标识符系统所涉及的其他利益相关方协调，以及发布风险评估方法。	ICANN 组织	中 - 高
2.4	ICANN 组织应在这个职位的职责说明中指出，此职务将负责所有与安全相关的预算项目，参与 ICANN 组织进行的所有与安全相关的合同谈判（例如，注册管理机构和注册服务机构协议、硬件和软件供应链，以及相关的服务水平协议），并代表 ICANN 组织签署所有与安全相关的合同条款。	ICANN 组织	中 - 高

SSR2 建议 3：提高 SSR 相关预算的透明度			
3.1	首席安全官（请参阅 SSR2 建议 2：设立相应的高级管理层职位，全面负责安全战略和战术以及风险管理）应代表 ICANN 组织每年两次向社群简要介绍 ICANN 组织的 SSR 战略、项目和预算，同时更新并发布年度预算概述。	ICANN 组织	高
3.2	ICANN 董事会和 ICANN 组织应确保，与 ICANN 组织履行 SSR 相关职能有关的特定预算项目符合特定的 ICANN 战略规划目标和宗旨。ICANN 组织应通过连贯一致的详细年度预算和报告流程来实施这些机制。	ICANN 董事会和 ICANN 组织	高
3.3	在战略规划周期内，ICANN 董事会和 ICANN 组织应创建、发布，并征询公众对有关成本以及 SSR 相关预算的详细报告的意见和建议。	ICANN 董事会和 ICANN 组织	高
SSR2 建议 4：改进风险管理流程和程序			
4.1	ICANN 组织应继续集中统一风险管理，明确阐述其安全风险管理框架，并确保该框架在战略上符合 ICANN 组织的要求和目标。ICANN 组织应明确相关的成功衡量标准以及评估方法。	ICANN 组织	高
4.2	ICANN 组织应采用并实施 ISO 31000“风险管理”标准，并通过适当的独立审计来验证实施情况。ICANN 组织应向社群提供审计报告，可以是修订后的版本。风险管理工作应纳入 BC 和 DR 计划和程序（请参阅 SSR2 建议 7：改进业务连续性和灾难恢复流程和程序）。	ICANN 组织	高
4.3	ICANN 组织应指定或任命一名专门负责安全风险管理的人员，该人员将向高级管理层安全负责人报告工作（请参阅 SSR2 建议 2：设立相应的高级管理层职位，全面负责安全战略和战术以及风险管理）。该人员应定期更新、报告安全风险记录，并指导 ICANN 组织的活动。发现的问题应纳入 BC 和 DR 计划和程序（请参阅 SSR2 建议 7：改进业务连续性和灾难恢复流程和程序）以及信息安全管理系统 (ISMS)（请参阅 SSR2 建议 6：遵守适当的信息安全管理系统和安全认证规定）。	ICANN 组织	高
SSR2 建议 5：遵守适当的信息安全管理系统和安全认证规定			
5.1	ICANN 组织应实施 ISMS，并由第三方按照行业安全标准（例如 ITIL、ISO 27000 系列标准、SSAE 18）对其运营责任进行审计和认证。计划应包括获得认证的路线图和里程碑日期，并注明未来有待持续改进的目标领域。	ICANN 组织	高

5.2	在 ISMS 的基础上，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纳入 ICANN 组织的安全与风险管理战略。	ICANN 组织	高
5.3	ICANN 组织应要求向 ICANN 组织提供服务的外部相关方遵守相关安全标准，并妥善记录对供应商和服务提供商展开的尽职调查。	ICANN 组织	高
5.4	ICANN 组织应与社群和更广泛的人群进行交流，通过清晰的报告展示 ICANN 组织在安全领域所做的工作和已取得的成就。如果这些报告能够提供信息，介绍 ICANN 组织是如何遵循最佳做法，并不断完善和持续优化用于管理风险、安全和漏洞的流程的，那么这些报告将非常有用。	ICANN 组织	高
SSR2 建议 6：SSR 漏洞披露和透明度			
6.1	ICANN 组织应积极推动签约方自愿采用 SSR 最佳做法和漏洞披露目标。如果自愿措施被证明不足以推动采用此类最佳做法和漏洞披露目标，那么 ICANN 组织应在合同、协议和谅解备忘录中列明实施最佳做法和漏洞披露目标的要求。	ICANN 组织	高
6.2	ICANN 组织应实施协调性弱点披露报告流程。关于 SSR 相关问题的披露和信息，例如任何签约方的数据外泄以及发现并向 ICANN 组织报告的关键漏洞，均应及时通知值得信赖的相关方（例如，受影响的或需要解决特定问题的相关方）。ICANN 组织应定期报告漏洞（至少每年一次），包括匿名的衡量标准并使用负责任的披露机制。	ICANN 组织	高
SSR2 建议 7：改进业务连续性和灾难恢复流程和程序			
7.1	ICANN 组织应根据 ISO 22301“业务连续性管理”制定适用于其自有或管辖的所有系统的业务连续性计划，并在计划中确定可接受的 BC 和 DR 时间表。	ICANN 组织	中 - 高
7.2	ICANN 组织应确保适用于公共技术标识符 (PTI) 运营（即，IANA 职能）的 DR 计划涵盖了可促进 DNS 安全与稳定的所有相关系统以及根区管理，且符合 ISO 27031 相关标准。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 (RSO) 密切合作，共同制定此计划。	ICANN 组织	中 - 高
7.3	同样，ICANN 组织也应根据 ISO 27031 相关标准制定适用于其自有或管辖的所有系统的 DR 计划。	ICANN 组织	中 - 高

7.4	ICANN 组织应为 ICANN 组织自有或管辖的所有系统建立一个新的灾难恢复站点，用于替代洛杉矶或库尔佩珀站点或增加一个永久性的第三站点。ICANN 组织应将这个新站点设在北美地区和美国领土之外的其他地方。如果 ICANN 组织选择替换其中一个现有站点，无论替换哪一个，ICANN 组织都应先确认新站点可以完全运行并且能够为 ICANN 组织处理这些系统的灾难恢复，然后再关闭要被替换的现有站点。	ICANN 组织	中 - 高
7.5	ICANN 组织应发布一份总体 BC 和 DR 计划和程序的摘要。这样做可以提高透明度和可信度，而不仅仅只是解决符合 ICANN 组织的战略目标和宗旨的问题。ICANN 组织应聘请外部审计人员来验证这些 BC 和 DR 计划是否合规。	ICANN 组织	中 - 高
SSR2 建议 8：在与签约方的谈判中维护并展现公共利益			
8.1	ICANN 组织应委托一个谈判小组（由不附属于签约方或不是由签约方聘请的滥用和安全领域专家组成）来代表非签约实体的利益，并与 ICANN 组织合作，双方本着诚信、公开透明的原则重新谈判签约方合同，主要目标是提高 DNS 的安全、稳定与弹性 (SSR) 以维护最终用户、企业和政府的利益。	ICANN 组织	中
SSR2 建议 9：监督并强制实施合规			
9.1	ICANN 董事会应指示合规团队监督并严格要求签约方遵守合同、基本协议、临时规范以及社群政策中关于现有和未来 SSR 以及滥用相关的义务。	ICANN 董事会	高
9.2	ICANN 组织应主动监督并强制要求注册管理机构和注册服务机构履行合同义务，以提高注册数据的准确性。这种监督和强制实施应包括验证地址字段，以及定期审核注册数据的准确性。ICANN 组织的强制合规工作应重点关注那些因提供不准确数据而每年受到向 ICANN 组织投诉或报告超过 50 起的注册服务机构和注册管理机构。	ICANN 组织	高
9.3	ICANN 组织应至少每年请外部人员对合规活动进行审计，并公布审计报告和 ICANN 组织对审计建议的回复，包括实施规划。	ICANN 组织	高
9.4	ICANN 组织应责成合规职能部门发布定期报告，列举他们缺少的工具，他们需要这些工具来支持 ICANN 组织作为一个整体，有效地利用合同杠杆来应对 DNS 中的安全威胁，包括需要更改合同条款的措施。	ICANN 组织	高

SSR2 建议 10：明确滥用相关术语的定义			
10.1	ICANN 组织应发布一个网页，明确 DNS 滥用的有效定义，即，适用的项目、文档和合同。定义应明确指出 ICANN 组织目前认为在其职权范围内通过合同和合规机制可以解决的安全威胁类型，以及 ICANN 组织认为属于其职权范围之外的安全威胁类型。如果 ICANN 组织使用其他类似术语（例如，安全威胁、恶意行为），那么 ICANN 组织应同时指明这些术语的有效定义，以及 ICANN 组织如何将这些术语与 DNS 滥用区分开。本页面应包含具体链接，指向与签约方签订的合同中各项与滥用相关的现有义务的摘要，包括应对滥用的相关程序和协议。ICANN 组织应每年更新此页面，注明最新版本的日期，并链接到具有相关发布日期的旧版本。	ICANN 组织	高
10.2	组建一个由员工提供支持的跨社群工作组 (CCWG)，负责确立一个流程来不断完善阻止 DNS 滥用的定义，至少每两年一次按照可预测的时间表（例如，隔年的一月份）更新一次 DNS 滥用的定义，在 30 个工作日内完成此流程。跨社群工作组应包括来自消费者保护、运营网络安全、学术界或独立网络安全研究机构、执法机构，以及电子商务领域的利益相关方。	ICANN 组织	高
10.3	ICANN 董事会和 ICANN 组织应在公共文档、合同、审核小组实施规划以及其他活动中一致地使用共识定义，并在出现此类使用情况时参考本网页。	ICANN 组织	高
SSR2 建议 11：解决 CZDS 数据访问问题			
11.1	ICANN 社群和 ICANN 组织应采取措施，以确保请求人员能够及时访问集中化域资料服务 (CZDS) 数据，不会遭受不必要的障碍，例如没有自动续订访问凭证。	ICANN 社群和 ICANN 组织	中
SSR2 建议 12：全面改进 DNS 滥用分析和报告工作，以实现透明度和独立审核			
12.1	ICANN 组织应创建一个由独立专家（即，没有财务利益冲突的专家）组成的 DNS 滥用分析咨询小组，对 DNS 滥用报告活动提出全面改进建议，将可操作的数据、验证、透明度和独立的可重复性分析作为最高优先级事项。	ICANN 组织	中
12.2	ICANN 组织应与数据提供商达成协议，允许进一步共享非商业用途的数据，特别是用于验证或需要进行同行评审的科学研究。这种特殊的免费非商业数据使用许可，可能会存在时间上的滞后，以免影响数据提供商的商业收入机会。ICANN 组织应在 ICANN 网站上发布所有数	ICANN 组织	中

	据共享合同条款。ICANN 组织应终止任何不允许对拦截清单背后的方法进行独立验证的合同。		
12.3	ICANN 组织应发布报告，揭示其域名最易造成滥用的注册管理机构和注册服务机构。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。	ICANN 组织	中
12.4	ICANN 组织应整理并发布注册管理机构和注册服务机构采取的措施报告，包括自愿行动和履行法律义务的做法，以便根据与使用 DNS 相关的适用法律对非法和/或恶意行为的投诉做出回应。	ICANN 组织	中
SSR2 建议 13：提高滥用投诉报告的透明度和问责制			
13.1	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。它将纯粹作为一个信息流入系统，ICANN 组织只收集和处理摘要和元数据，包括时间戳和投诉类型（分类）。所有通用顶级域 (gTLD) 都必须使用该系统；每个国家和地区顶级域 (ccTLD) 自愿参与。此外，ICANN 组织还应与所有 ccTLD 共享滥用报告（例如，通过电子邮件）。	ICANN 组织	高
13.2	ICANN 组织应以允许独立第三方分析关于 DNS 投诉类型的形式发布其收到的投诉数量。	ICANN 组织	高
SSR2 建议 14：制定临时规范，提高基于证据的安全性			
14.1	ICANN 组织应制定临时规范，要求所有签约方将已修订的 DNS 滥用报告中确定为滥用的域名所占百分比保持在合理范围和已发布的阈值之下（请参阅 SSR2 建议 13.1）。	ICANN 组织	高
14.2	为促进反滥用行动，ICANN 组织应根据关于独立审核域名数据和拦截清单方法的 SSR2 建议 12.2，向签约方提供其域名组合中被认定为滥用的域名列表。	ICANN 组织	高
14.3	如果与滥用活动相关的域名数量达到 SSR2 建议 14.1 中所述的已发布阈值，ICANN 组织应展开调查以确认数据和分析的准确性，然后向相关方发出通知。	ICANN 组织	高
14.4	ICANN 组织应给签约方 30 天时间，供对方将滥用域名的比例降低到阈值以下或证明 ICANN 组织的结论或数据存在问题。如果签约方在 60 天内未能纠正错误，ICANN 合同合规部应开始取消认证流程。	ICANN 组织	高

14.5	ICANN 组织应考虑提供财务激励措施：域名组合中滥用域名比例低于特定百分比的签约方，将有机会获得适当程度减免应付交易费用的奖励。	ICANN 组织	高
SSR2 建议 15：启动 EPDP 以提高基于证据的安全性			
15.1	制定临时规范后（请参阅 SSR2 建议 14：制定临时规范，提高基于证据的安全性），ICANN 组织应建立由员工提供支持的快速政策制定流程 (EPDP) 以制定反滥用政策。EPDP 志愿者应代表 ICANN 社群，使用 gTLD 注册数据临时规范 EPDP 团队章程中的号码和分配作为模板。	ICANN 组织	高
15.2	EPDP 应参考 SSR2 建议 10.2 中拟议的 CCWG 基本定义。该政策框架应明确定义针对不同类型的滥用行为的适当对策和补救措施，签约方采取措施的时间框架（例如滥用报告/响应报告时间表），以及在出现违反政策的情况下，ICANN 合同合规部可采取的强制措施。如果任何签约方有包庇滥用行为的方式和做法，ICANN 组织应坚持要求终止合同。结果应包括建立一个机制，每两年对滥用相关的基准和合同义务更新一次，通过一个不超过 45 个工作日的流程来完成这项工作。	ICANN 组织	高
SSR2 建议 16：隐私要求和 RDS			
16.1	ICANN 组织应在其网站上提供一致的交叉引用，以提供关于隐私和数据管理主题的所有举措（过去、现在和计划中）的一致且易于查找的信息，特别是注册目录服务 (RDS) 相关信息。	ICANN 组织	中
16.2	ICANN 组织应在合同合规职能部门内建立专门小组，负责深入了解隐私要求和原则（例如，收集限制、数据资格、目的规范以及数据披露的安全保护措施），并在 RDS 框架下促进执法需求，因为社群已修订和批准了该框架（另请参阅 SSR2 建议 11：解决 CZDS 数据访问问题）。	ICANN 组织	中
16.3	ICANN 组织应定期审计注册服务机构隐私政策履行情况，确保注册服务机构制定了用于处理侵犯隐私行为的流程。	ICANN 组织	中
SSR2 建议 17：衡量域名冲突			
17.1	ICANN 组织应制定框架，总结各类域名冲突的性质和发生频率以及所产生的问题。该框架应包括具体衡量标准和若干机制，用于衡量控制性中断在多大程度上可成功识别并消除域名冲突。可通过启用受保护的域名冲突披露实例这一机制来提供支持。此框架应允许适当处理敏感数据和安全威胁。	ICANN 组织	中

17.2	ICANN 社群应制定一项明确的政策，用于避免和处理与新 gTLD 相关的域名冲突，并在下一轮 gTLD 相关工作启动之前实施该政策。ICANN 组织应确保由与 gTLD 扩展没有财务利益关系的相关方来评估该政策。	ICANN 社群和 ICANN 组织	中
SSR2 建议 18：为政策辩论提供信息			
18.1	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 安全与隐私讨论会、运营安全会议，以及事故响应和安全团队论坛 (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。	ICANN 组织	低
18.2	ICANN 组织应确保此类报告中包含可能与可行措施建议相关的观察结果（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的更改），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。	ICANN 组织	低
18.3	ICANN 组织应确保这些报告中还包含开展其他研究的建议，以确认经过同行评审的研究结果，其中应介绍社群需要哪些数据才能开展其他研究，以及 ICANN 组织如何为代理提供协助以通过 CZDS 来访问此类数据。	ICANN 组织	低
SSR2 建议 19：完成 DNS 回归测试套件的开发工作			
19.1	ICANN 组织应完成 DNS 解析程序行为测试套件的开发工作。	ICANN 组织	低
19.2	ICANN 组织应确保实施并维护这项继续针对不同配置和软件版本进行功能测试的性能。	ICANN 组织	低
SSR2 建议 20：用于指导密钥轮转的正式程序			
20.1	ICANN 组织应通过正式流程建模工具和建模语言的支持，制定所需的正式流程，以详细说明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（例如程序、有限状态机 (FSM)）以征询公众意见，并且 ICANN 组织应收集社群反馈意见。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（即，相同的频率），以便	ICANN 组织	中

	ICANN 组织能够及时运用已吸取的经验教训对流程进行调整。		
20.2	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密钥签名密钥 (KSK) 轮转流程运行桌面演练。	ICANN 组织	中
SSR2 建议 21：提高与 TLD 运营商的通信安全性			
21.1	ICANN 组织和 PTI 运营部门应加快实施新的根区管理系统 (RZMS) 关于针对请求的更改进行身份认证和授权的安全措施，并为 TLD 运营商提供利用这些安全措施的机会，特别是 MFA 和加密电子邮件。	ICANN 组织和 PTI	中
SSR2 建议 22：服务衡量标准			
22.1	对于 ICANN 组织权威管辖的每项服务（包括根区服务、gTLD 相关服务以及 IANA 注册管理机构），ICANN 组织应创建一个统计信息和衡量标准列表来反映该项服务的运营状态（例如，可用性以及响应性），并在 icann.org 网站的单个页面上，例如，Open Data Platform（开放数据平台）下发布这些服务、数据集和衡量标准的目录。ICANN 组织应对这些服务中的每一项进行衡量，作为去年和纵向总结（以阐释基准行为）。	ICANN 组织	低
22.2	ICANN 组织应每年征询社群对这些衡量标准的反馈意见。在每次报告发布后，应审议并公开总结相关反馈，并纳入后续报告。用于衡量这些报告结果的数据和相关方法应妥善存档，并公开发布以促进重复利用。	ICANN 组织	低
SSR2 建议 23：算法轮转			
23.1	PTI 运营部门应更新 DNSSEC 实践声明 (DPS)，以允许从一种数字签名算法过渡到另一种数字签名算法，包括预期的从 RSA 数字签名算法过渡到其他算法或未来的后量子算法，这些算法可提供同等或更高的安全性，并且可保持或增强 DNS 的弹性。	PTI	中
23.2	鉴于根区 DNSKEY 算法轮换是一个非常复杂且敏感的流程，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。	PTI	中

SSR2 建议 24：提高 EBERO 流程的透明度和改进端到端测试			
24.1	ICANN 组织应使用测试计划按预定时间间隔（至少每年一次）协调整个 EBERO 流程的端到端测试，测试计划包括用于测试的数据集、进展状态以及截止日期，同时应提前与 ICANN 签约方协调，以确保所有例外条款得到执行并公布测试结果。	ICANN 组织	中
24.2	ICANN 组织应在 EBERO 网站上提供链接，以便用户更容易找到《共同过渡流程手册》。	ICANN 组织	中

2. 优先顺序

SSR2 审核小组已根据《ICANN 2021-2025 财年战略规划》及其目标和宗旨调整了所有 SSR2 建议。[6]审核小组删除了本报告中与战略规划明显不一致的建议。SSR2 审核小组提出的所有建议均符合 ICANN 组织的战略规划，因此这些建议都非常重要。

SSR2 审核小组使用了一款在线调查工具（基于互联网的解决方案 Qualtrics），供所有小组成员就本报告中每组建议的优先级发表意见。[7]这项调查允许按五个等级（非常低优先级、低优先级、中等优先级、高优先级，以及非常高优先级）对每组建议的优先级进行排名。

审核小组认为，这 24 组建议中有 27 项具体建议应被视为高优先级建议，其中大部分建议涉及 ICANN 组织的内部安全管理和反滥用举措。9 项建议为中高优先级。18 项建议（主要来自全球 DNS 部门）为中等优先级，其余 8 项建议为较低优先级。

[6] 请参阅附录 G：了解 SSR2 建议与《ICANN 2021-2025 财年战略规划》和《ICANN 章程》的关系。
[7] 请参阅 https://www.qualtrics.com/。