ICANN 的说明：

以下执行摘要由安诺析思国际咨询 (Analysis Group) 公司（SSAC 审核的独立审核人）作为其最终报告的简介提交。

独立审核人报告的权威版本原件为英文，在线网址为：https://www.icann.org/en/system/files/files/ssac-review-final-17dec18-en.pdf。

针对 ICANN 安全与稳定咨询委员会的独立审核：
执行摘要

已将报告呈报给互联网名称与数字地址分配机构 (ICANN)

作者：什洛莫 • 赫什科普 (Shlomo Hershkop) 博士、
克里斯托弗 • 洛普 (Christopher Llop)、
格雷格 • 拉夫特 (GREG RAFERT) 博士
史蒂夫 • 韦伯 (Steve Weber) 教授[1、2]

2018 年 12 月 17 日

[1] 什洛莫 • 赫什科普博士现任 Allure 安全技术公司的工程总监，曾在宾夕法尼亚大学和纽约市哥伦比亚大学担任过 15 年的兼职教授。史蒂夫 • 韦伯教授是加州大学伯克利分校中心长期网络安全中心 (CLTC) 的教学主任和联合创始人，该中心致力于根据互联网及其未来的长期愿景来开发和设计网络安全研究和实践。格雷格 • 拉夫特（副总裁）和克里斯托弗 • 洛普（助理）是安诺析思国际咨询公司（一家国际经济、金融和战略咨询公司）的员工。

[2] 作者要感谢 SSAC RWP 在审核流程中的全面参与，感谢 SSAC 与我们一起召开了公开会议，感谢 ICANN 的 MSSI 在访谈和会议协调方面提供的大量帮助。另外，我们也感谢所有抽时间接受访谈、调查，或是针对评估报告或最终报告草案提供意见的人员，感谢安诺析思国际咨询公司的阿尔穆德纳 • 阿尔塞卢斯（Almudena Arcelus，负责人）和奥斯汀 • 贝尔（Austin Bell，高级分析师）在研究、数据分析和报告审核方面提供的帮助。

I. 简介

安全与稳定咨询委员会 (SSAC) 的工作是就与互联网名称和地址分配系统的安全性和完整性相关的事宜向 ICANN 社群和 ICANN 董事会提供建议。ICANN 章程规定，应该至少每 5 年对 SSAC 举行一次独立审核。[3]根据此要求，我们的审核包括以下评估：

- SSAC 是否在 ICANN 结构中有持续存在的必要。
- SSAC 履行其职责的效率，并确定是否有必要对其架构或运营进行任何调整来改善其工作效率。
- SSAC 作为一个整体对更广泛的 ICANN 社群、其组织、委员会、选区和利益相关方团体的负责情况如何。
- SSAC 此前审核的实施状况。[4]

本报告根据以下内容提供了调查结果和建议：对 ICANN 社群成员的访谈和调查、对 SSAC 的观察，以及有关在 ICANN 内部及与其他非营利和志愿者组织的广泛合作以提高其效率方面的经验。此外，“评估报告”于 2018 年 6 月 20 日发布，在编写本报告时所反映的反馈意见是通过 ICANN 第 62 届会议、公共网络研讨会和公共评议期从 ICANN 社群征集而来的。[5]

最终报告草案于 2018 年 10 月 15 日发布，并且已公开征求公众意见，截止时间为 2018 年 12 月 3 日。[6]最终报告草案已在 ICANN 第 63 届会议上提交讨论，并于 2018 年 11 月 20 日通过网络研讨会进行讨论。对独立审核人来说，此公共评议期的对话和意见是非常有帮助的，我们非常感谢那些抽出时间在整个审核流程中提供帮助的人员，其中包括从接受访谈和调查的人员到那些以书面报告的形式提供反馈意见的人员。

我们对 SSAC 的评估是在 2018 年 2 月到 7 月之间进行的。此次评估发现，SSAC 是一个富于成效的组织，但在某些领域，其仍有改进的余地。我们的报告提供了 22 项调查结果（在此报告为 23 项调查结果，以方便讨论），其涉及到一系列广泛的主题领域，其中包括：

---

[3] ICANN 章程，*ICANN*，第 4 条，第 4 款，位于 https://www.icann.org/resources/pages/governance/bylaws-en#VII-1，访问时间：2018 年 5 月 1 日。

[4] ICANN 关于审核 ICANN 安全与稳定咨询委员会提案征询的概况，*ICANN*，2017 年，位于 https://www.icann.org/en/system/files/files/rfp-ssac-review-07jul17-en.pdf，访问时间：2018 年 5 月 20 日。

[5] 我们由衷感谢在公共评议会议、网络研讨会和公共评议期提出意见的所有人，包括提供书面意见的非利益相关方团体。

[6] SSAC 审核网站上提供有 6 条公众意见和一份公共评议报告。“第二次安全与稳定咨询委员会审核 (SSAC2) 的最终报告草案”，位于 https://www.icann.org/public-comments/ssac-review-final-2018-10-15-en，访问时间：2018 年 12 月 13 日。

- SSAC 的工作效率，例如要求 SSAC 完成的工作量和 SSAC 已完成的工作量，了解 ICANN 董事会实施 SSAC 建议的现有机制，以及提出 SSAC 建议并采取措施的时间。
- SSAC 与其他 SO/AC 和更广泛 ICANN 社群之间的关系和相互联系，其中包括透明度问题。
- SSAC 的现有成员和结构，包括其规模、成员招聘和任期限制。
- SSAC 先前审核的实施状态，其结果已于 2009 年发布。

我们根据评估调查结果在本报告中提供了总共 30 项建议。

每个调查结果都会附有相关的建议（如果有的话）。有时候，调查结果和建议之间并不存在完美的一对一关系，因为可能有多个调查结果与一个建议相关，同时多项建议可能会寻求解决一个调查结果。

报告第二部分提供了 SSAC 的背景知识，第三部分讨论了我们对 ICANN SSAC 进行独立审核时所遵循的方法。报告的第四部分到第七部分详细介绍了我们的调查结果和建议。以下是对建议的概述，这些建议在本报告中按章节分组列出。

第四部分涉及 SSAC 的持续存在目的。

1. SSAC 在 ICANN 中具有明确的持续存在的目的。它应该继续作为咨询委员会存在。

   大家普遍认为，对 ICANN 的整体使命来说，SSAC 是非常重要的。

第五部分涉及 SSAC 如何提出建议以及如何将建议提供给 ICANN 董事会。

2. SSAC 应确保向 ICANN 董事会提供的每份咨询或报告都包括一份简要的摘要，用容易理解的术语概括主题或问题，并列出具有独特编号建议的主要调查结果。

   这将会使个别建议更容易确定并追踪到解决方法，从而可帮助董事会解释并实施 SSAC 建议。

3. 在提供建议时，SSAC 应确保在将概要和整个文档提交给董事会之前，董事会联络人会对其进行审核并提供反馈。SSAC 应主动与 SSAC 董事会联络人讨论谈话要点以及董事会做出回应的可能时间。

   这将有助于确保建议的措辞易于理解，并且能方便地将建议付诸实施，同时有助于 SSAC 预测董事会的建议审核时间将如何与其竞争的优先事项相互影响。

4. SSAC 董事会联络人应与 ICANN 董事会和 ICANN 员工合作，确保董事会行动请求注册 (ARR) 充分获取所需信息，以了解从建议提出到实施期间建议的具体状态。

   这将有助于更简单和更省时地确定任何尚待 ICANN 董事会回应或实施的建议的状态。

5. SSAC 应定期审核提供给 ICANN 董事会的以往建议和将来建议的实施状况，以确保所有的行动事项均列在 ARR 中。当建议尚未得到解决或进展不明确时，SSAC 应通过董事会联络人对 ICANN 董事会进行跟进。

   使用更新后的 ARR，SSAC 应该能够相对容易地审核并检查提供给 ICANN 董事会的任何建议的状态。

6. 对于时间敏感问题，SSAC 应该制定流程和工作期限，同时将其他 ICANN 实体的决策时间表考虑在内。SSAC 应与 SSAC 员工合作，以确保设定内部截止期限，从而尽可能合理地满足外部截止日期。

   在合理而又不影响提供有效建议的情况下，SSAC 应继续努力使其工作与 ICANN 截止期限保持一致。

7. SSAC 应制定一个流程，以尽可能为董事会提供一个“快速查看”特定问题的方法。这种“快速查看”可能并不是以共识为基础流程的结果，但其可以公开不同的意见。

   这有助于 ICANN 董事会更快、更好地理解某些特定问题。当“快速查看”请求不合理时，SSAC 的联络人可以与 ICANN 董事会合作对 SSAC 提出的请求或问题加以改进。

8. SSAC 应正式确定一项年度流程，旨在确定研究重点，并确定短期和中期内出现的有关安全、稳定与弹性 (SSR) 问题。

   这将使 SSAC 能够在短期（1 年）和更长的中长期（5 年）时间范围内规划研究目标和成员需求。

9. SSAC 的年度优先事项设置和突发威胁识别工作中确定的任务所需的技能应纳入 SSAC 的成员资格和招聘流程。

   SSAC 即将推出的优先事项可以根据当前成员的兴趣、技能和可用性来进行评估。委员会可以帮助确定是否应将新成员或受邀来宾纳入 SSAC，以应对日后需求。

10. SSAC 应明确告知其围绕主题选择做出决定的原因，并与 ICANN 内的其他成员对其进行重点关注。同时应将新的请求与当前的优先事项设置进行比较，并针对这一事宜进行相应的沟通。

    SSAC 处理了许多请求并完成了大量的工作。在对 SSAC 提出更多要求时，以及在考虑满足请求所需的权衡和资源时，可以参考一组清晰的研究优先事项设定。

11. 当需要额外资金、资源或访问外部承包商以在所需的时间安排内或在所需的规模上实现某个项目时，SSAC 应继续与 ICANN 董事会接洽。

    此举可使 ICANN 改进请求或协助 SSAC 获取所需资源。

12. SSAC 应考虑是否可以为网络安全或数据分析项目的研究生提供实习机会，以获得有关研究或特定工作产品方面的帮助。此外，SSAC 应继续努力，在适当时利用 ICANN 技术人员的协助。

    就像 SSAC 目前的志愿者一样，有能力的学生通常有兴趣自愿与专家合作来积累经验。某些任务也可以通过采用带薪或无薪实习来委派。

13. SSAC 应与 ICANN 员工合作，以获取用于 SSAC 分析的专用、安全的数据存储位置。

    集中式存储有助于随着时间推移来组织和维护数据。

第六部分涉及到 SSAC 与 SO/AC 和 ICANN 社群的整合。

14. SSAC 负责针对有关互联网命名和地址分配系统安全性和完整性的事宜，向 ICANN 董事会和社群提供建议。为了有效地实现这一点，SSAC 需要了解 ICANN 内部正在制定的政策。我们建议 SSAC 为每个愿意拥有外派代表的 SO/AC 指定一名代表。由于 SSAC 已肩负着巨大的责任，因此这些职位应架构在尽可能少地向其叠加负担的基础之上。

    这种方式可以为与每个 SO/AC 的开放式沟通提供了一种机制，通过该机制，SSAC 可以随时了解 SO/AC 的活动和 PDP 流程，并且可以帮助其了解可能在未来变得非常重要的 SSR 问题类型。当 SSAC 的建议和意见可能对 SO/AC 产生影响时，他们也可以帮助 SSAC 主动进行沟通。

15. 如果时间允许，SSAC 应该继续让成员以个人的身份参与具有 SSR 相关组成部分（例如 SSR2）的大量跨 ICANN 部门工作。

    这样做能够让 SSAC 的成员在他们可以发挥作用的地方运用其专业知识，并使 SSAC 与更广泛的 ICANN 计划保持持续联系。

16. 在制定每个 SAC 系列文档的流程中，SSAC 应该针对以下内容展开明确的讨论：可能受影响的各方；是否应该咨询受影响方以获得反馈；以及针对 SSAC 打算发布关于特定主题的文档，是否应该予以通知。

征求反馈意见可以为 SSAC 提供额外信息，以在提出建议时加以考虑，也可以协助 SSAC 考虑如何将其建议付诸实施，并增进潜在受影响方对 SSR 的了解。

17. SSAC 的管理委员会应在每届 ICANN 会议的前一个月向 ICANN 的 SO/AC 领导层发送一封电子邮件更新，并附上指向 SSAC 网站上与 SSAC 文档/程序有关的链接。

    那些可在SO/AC 中共享的简短通信使得SSAC 更具透明度，并且可在ICANN 会议临近时首先考虑SSR 问题。

18. SSAC 应在短期内在线发布一些特定的其他资料，以强化信息并提高透明度。然后，SSAC 管理委员会应对 SSAC 网站进行年度审查，以确定是否应该提供其他内容或是否应对网站进行重组。

    定期改进网站可以提高透明度，并且可以为成员招聘提供帮助。

19. SSAC 应该直接对 ICANN 董事会负责，并通过董事会对更广泛的 ICANN 社群负责。

    SSAC 当前的问责机制是适当的。

第七部分涉及 SSAC 的规模、成员资格以及任期和期限。

20. SSAC 成员的当前数量适中。SSAC 应继续努力，结合以下各招聘点，以确保其成员参与。

    SSAC 应该每年都有一定的人员流动，以便可以提供新的想法和观点，同时也要保留活跃成员的专业知识。

21. SSAC 应该每年都制定正式的招聘计划，其中包括目标、潜在招聘目标、要参与的会议、为潜在候选者发送消息，以及任何其他被认为有用的项目。同样，SSAC 应保留一份可能的未来成员的名单，即便这些人当前并不适合在 SSAC 任职。

    正式的招聘计划可帮助 SSAC 提高其人才管道的稳健性，缓解退休成员的过渡，反映所需技能和多样性以实现更多中期目标，以及根据工作量的增加来扩大其网络。

22. SSAC 应与 ICANN 董事会合作，争取活动资金以便在 ICANN 会议之外可以每年参加两到三次主要安全会议，在这些会议上，成员可能会遇到新的感兴趣的申请人。

    在学术和专业会议中，将有机会与SSR 相关领域内的著名专家和新兴专家会面，他们可能会作为未来的 SSAC 成员或特邀嘉宾提出一些有用的新观点。它还有助于提高地理多样性。

23. SSAC 成员委员会应该制定一份学术或其他机构的名单，其中包括 SSR 相关领域内的研究成果。成员委员会应将这份列表保持为最新，并考虑专业学者是否可以作为特邀嘉宾或正式的 SSAC 成员来提供有用的观点。

    在相关领域工作的专业学者可能有兴趣与 SSAC 合作。与学术机构的联系也可以作为个人协助SSAC 工作的支线。

24. SSAC 应继续努力招募具有强大技术背景同时兼具法律/政策专业知识的人员。应该在每年的招聘计划制定过程中针对具有法律、政策和执法专业知识的个人需求进行讨论。

    尽管 SSAC 当前的成员在法律、政策和执法背景方面都具有丰富经验，但重要的是要继续将其作为规划SSAC 招聘时所考虑的标准。

25. SSAC 应努力招募具有强大技术背景的人员，同时这些人员也应该体现广泛的地理区域和合理的性别平衡。关于如何实现这一点的讨论应该纳入到每年的招聘计划制定过程中。

    在可以为 SSAC 获得多样性和所需的技术专业知识时，应该制定流程以最大限度地提高这种可能性。

26. SSAC 的成员审核流程应包括 SSAC 外部联络人和代表的年度审核流程。

    这种非正式审核将向 SSAC 的外部接口提供反馈，以帮助他们确定哪些措施能够发挥作用。

27. SSAC 领导层的任期期限应为两年、三年。SSAC 不应对非领导成员施加任何任期限制。

    除了SSAC 主席的任期限制之外，这与SSAC 的当前任期限制相符。

28. SSAC 应与 ICANN 董事会合作更新 ICANN 章程，以便对 SSAC 主席执行任期限制。

    更新完成后，SSAC 应该根据上面的描述限制其主席的任期。

29. SSAC 应保持其当前的流程和活动，公开潜在利益冲突，无论是在个人层面还是作为个人团体。它还应更新其在线的利益披露声明，明确阐明最后一次向每位成员提交披露的时间。

    在像 SSAC 这样的组织中，不可能确保每个个人之间完全不存在利益冲突。相反，SSAC 需要在个人团体中进行内部检查，以确保冲突得到了解决，并且不会影响组织制度上的决定。

第八部分涉及 SSAC 先前的审核实施情况和自我完善的持续努力。

30. SSAC 应继续培养和发扬重视自我完善的 SSAC 文化，包括在正式审核之间。

> *有效的组织不仅要在正式流程中学习和改进，还要在积累经验时不断反思。这种持续改进使组织能够即时学习并且可以稳健地进行*变革*。*

除上述这些建议之外，我们注意到在管理工作时，SSAC 面临着一些紧张局面。例如，虽然技术卓越是 SSAC 可信度的基础，而卓越性与 SSAC 的共识流程紧密相关，但有时这可能与更广泛、更快速地与非技术成员进行沟通的需要相冲突。在将 SSAC 所讨论主题的外部透明度与不通知攻击者潜在安全风险的有责披露必要性之间进行平衡，或者在平衡组织灵活性和有时需要进行良好定义的正式流程时，也会出现类似的紧张局面。建议是在考虑平衡这些紧张局面的情况下提出的，正如本报告中进一步讨论的那样。