Note from ICANN:

The following executive summary was submitted as introduction to its final report by Analysis Group, independent examiner of the SSAC Review.

The authoritative version of the independent examiner's report is the English original, online at https://www.icann.org/en/system/files/files/ssac-review-final-17dec18-en.pdf .

Independent Review of the ICANN Security and Stability Advisory Committee:

Executive Summary

Report Prepared for the Internet Corporation for Assigned Names and Numbers (ICANN)

By Dr. Shlomo Hershkop, Christopher Llop, Dr. Greg Rafert, Professor Steve Weber[1,2]

December 17, 2018

[1] Dr. Shlomo Hershkop is the Director of Engineering at Allure Security Technology, Inc., and previously served for 15 years in roles as Adjunct Professors at the University of Pennsylvania and at Columbia University in the City of New York. Professor Steven Weber is the faculty director and a cofounder of UC Berkeley's Center for Long Term Cybersecurity (CLTC), an organization focused on developing and shaping cybersecurity research and practice based on a long-term vision of the Internet and its future. Greg Rafert (Vice President) and Christopher Llop (Associate) are employees of Analysis Group, Inc., an international economic, financial, and strategy consultancy.

[2] The authors would like to thank the SSAC RWP for its thoughtful participation in the review process, the SSAC for opening meetings to us, and ICANN's MSSI for extensive help in interview and meeting coordination. We also thank all who have taken the time to be interviewed, surveyed, or provide commentary on the Assessment Report or Draft Final Report, and thank Almudena Arcelus (Principal) and Austin Bell (Senior Analyst) at Analysis Group, Inc. for assistance in research, data analysis, and report review.

I. Introduction

The Security and Stability Advisory Committee (SSAC) advises the ICANN community and the ICANN Board of Directors (ICANN Board) on issues concerning the security and integrity of the Internet's naming and address allocation systems. The ICANN Bylaws stipulate that the SSAC be independently reviewed at least once every five years.[3] In accordance with this requirement, our review includes an assessment of:

- Whether the SSAC has a continuing purpose within the ICANN structure.
- How effectively the SSAC fulfills its purpose and whether any change in structure or operations is needed to improve effectiveness.
- The extent to which the SSAC as a whole is accountable to the wider ICANN community, its organizations, committees, constituencies, and stakeholder groups.
- The implementation state of the SSAC's prior review.[4]

This report provides findings and recommendations based on interviews with, and a survey of, ICANN community members, our observations of the SSAC, and our experience with ICANN and extensive work with other nonprofit and volunteer-based organizations to improve their effectiveness. In addition, an "Assessment Report" was published on June 20, 2018, and feedback reflected upon in the preparation of this report was solicited from the ICANN community via a public session at ICANN62, a public webinar, and a public comment period.[5]

A draft final report was released on October 15, 2018, and was open for public comment through December 3, 2018.[6] The draft final report was presented for discussion in person at ICANN63 and via webinar on November 20, 2018. The conversations and comments from this public comment period were helpful to the Independent Reviewer, and we would like to thank those who took the time to assist with the entire review process, from those interviewed and surveyed, to those who provided feedback on the written reports.

Our assessment of the SSAC was conducted from February through July of 2018. That assessment found the SSAC to be a productive and effective organization, with room to improve in certain

[3] ICANN Bylaws, *ICANN*, Article 4, Section 4, available at https://www.icann.org/resources/pages/governance/bylaws-en#VII-1, accessed on May 1, 2018.

[4] ICANN An Overview of the Request for Proposal for the Review of the ICANN Security and Stability Advisory Committee, *ICANN*, 2017, available at https://www.icann.org/en/system/files/files/rfp-ssac-review-07jul17-en.pdf, accessed on May 20, 2018.

[5] We would like to thank all those who commented during the public comment session, webinar, and period, including the Non-Commercial Stakeholder Group which provided written comments.

[6] Six public comments and a Report of Public Comments are available on the SSAC Review Website. "Draft Final Report of The Second Security and Stability Advisory Committee Review (SSAC2), available at https://www.icann.org/public-comments/ssac-review-final-2018-10-15-en, accessed December 13, 2018.

areas. Our report provided 22 findings (reported here as 23 findings for convenience of discussion) across a broad set of topic areas, including:

- The effectiveness of the SSAC, such as the amount of work asked of and accomplished by the SSAC, the mechanisms in place to understand the implementation of SSAC's advice by the ICANN Board, and the timing with which the SSAC's advice is provided and acted upon.
- The relationship and interconnectedness between the SSAC and both other SO/ACs and the broader ICANN Community, including on issues of transparency.
- The existing membership and structure of the SSAC, including its size, membership recruitment, and term limits.
- The implementation state of the SSAC's prior review, the results of which were released in 2009.

We provide in this report a total of 30 recommendations that are based on our assessment findings.

Each finding is presented followed by its associated recommendations, if any. At times, there is not a perfect one-to-one relationship between findings and recommendation, as multiple findings may relate to one recommendation, and multiple recommendations may seek to address a single finding.

Section II provides background on the SSAC and Section III discusses the methodology we followed for our independent review of ICANN's SSAC. Sections IV through VII of the report detail our findings and recommendations. Below, is an overview of our recommendations, listed in groups by section of this report in which they appear.

Section IV relates to the continuing purpose of the SSAC.

1. The SSAC has a clear continuing purpose within ICANN. Its existence as an Advisory Committee should continue.

   The SSAC is widely acknowledged to be very important to the overall mission of ICANN

Section V relates to the SSAC's advice generation and provision of advice to the ICANN Board.

2. The SSAC should ensure that each advisory or report provided to the ICANN Board includes a high-level summary that outlines the topic or issue in easily understandable terms and lists the key findings with uniquely numbered recommendations.

   This will assist the Board in interpreting then implementing SSAC advice by making individual recommendations easier to identify and track through to resolution.

3. When providing advice, the SSAC should ensure that the Board Liaison reviews and provides feedback on both the summary and full document before submission to the

Board. The SSAC should proactively discuss talking points and potential Board response timing with the SSAC Board Liaison.

This will help ensure recommendations are phrased in a way that can be understood and acted upon expediently, and will help the SSAC to predict how the Board's advice review timing may interact with its competing priorities.

4. The SSAC Board Liaison should work with the ICANN Board and ICANN Staff to ensure that Board Action Request Register (ARR) adequately captures the information required to understand the status of advice from when it is given through its implementation.

   This will make it easier and less time-intensive to identify the status of any recommendation that is pending ICANN Board response or implementation.

5. The SSAC should periodically review the implementation state of past and future advice provided to the ICANN Board to ensure that all action items are listed in the ARR. The SSAC should follow-up with the ICANN Board via its Board Liaison when advice has not yet been addressed or when progress is unclear.

   Using the updated ARR, the SSAC should be able to review then check in on the status of any recommendation provided to the ICANN Board with relative ease.

6. For time sensitive issues, the SSAC should establish process and work deadlines that take into account the decision timelines of other ICANN entities. The SSAC should work with SSAC staff to ensure internal deadlines are set up to make meeting external deadlines as possible as reasonable.

   The SSAC should continue to endeavor to align its work with ICANN deadlines where reasonably possible, without compromising the provision of sound advice.

7. The SSAC should develop a process to, when possible, provide a "quick look" at a particular issue for the Board. Such "quick looks" might not be the result of a consensus-driven process, but rather would disclose differing opinions.

   This will help the ICANN Board better understand certain issues more quickly. When a "quick look" request is unreasonable, the SSAC's Liaison can work with the ICANN Board to refine the request or questions asked of the SSAC.

8. The SSAC should formalize an annual process geared towards setting research priorities and identifying relevant emerging security, stability, and resiliency (SSR) threats in the short- and medium-term.

   This will allow the SSAC to plan research goals and membership needs around both a short- (1-year) and more medium-term (5-year) time horizon.

9. The skills needed for tasks identified in the SSAC's annual priority setting and emerging threat identification exercise should feed into the SSAC's membership and recruitment processes.

The SSAC's upcoming priorities can be assessed against current member interest, skills, and availability. The Membership Committee can help determine if new members or Invited Guests could be brought in to the SSAC for upcoming needs.

10. The SSAC should explicitly communicate the reasons for its decisions around topic selection and focus with others in ICANN. New requests should be compared to the current set of priorities and communicated about accordingly.

    The SSAC fields many requests and completes a large amount of work. A well-articulated set of research priorities can be referred back to when considering tradeoffs or resources needed to fulfill requests when more is asked of the SSAC.

11. The SSAC should continue to approach the ICANN Board when additional funding, resources, or access to external contractors may be required to achieve a project in the desired timeline or at the desired scale.

    This enables the ICANN Board to either refine requests or to assist the SSAC in obtaining required resources.

12. The SSAC should consider whether an internship can be offered to graduate students in cybersecurity or data analytics programs for assistance with research or specific work products. In addition, the SSAC should continue to endeavor to leverage the assistance of ICANN's technical staff when it is appropriate to do so.

    Much like the SSAC's current volunteers, highly capable students are often interested in volunteering time to work with experts and gain experience. Certain tasks may be delegable via either paid or unpaid internships.

13. The SSAC should work with ICANN Staff to obtain a dedicated, secure, data storage location for use in SSAC analyses.

    Centralized storage helps to organize and maintain data over time.

Section VI relates to the SSAC's integration with SO/ACs and the ICANN community.

14. The SSAC advises the ICANN Board and Community on matters relating to the security and integrity of the Internet's naming and address allocation systems. To do this effectively, the SSAC needs to be aware of policymaking that is ongoing within ICANN. We recommend the SSAC designate an outward representative to each SO/AC that is willing to have one. These roles should be structured to add minimal burden to the SSAC's already large set of responsibilities.

    An open line of communication with each SO/AC provides a mechanism by which the SSAC can keep apprised of the activities and PDP processes of SO/ACs, and can help it understand the types of SSR issues that may become important down the road. They also can help the SSAC communicate proactively when its advice and recommendations may affect an SO/AC.

15. As time availability allows, the SSAC should continue to have members involved as individuals in large, cross-ICANN efforts that have SSR-related components, such as the SSR2.

    Doing so will enable the SSAC's members to leverage their expertise where useful and keep the SSAC more continuously connected with wider ICANN initiatives.

16. In the process of developing each SAC-series document, the SSAC should explicitly discuss who affected parties may be and whether or not affected parties should be consulted for feedback or should be notified that the SSAC plans to publish a document on a given topic.

    Soliciting feedback can give the SSAC additional information to consider when generating advice, assist the SSAC in considering how its advice may be put into action, and increase SSR awareness within the potentially affected party.

17. The SSAC's Administrative Committee should provide an email update to the leadership of ICANN's SOs/ACs one month prior to each ICANN meeting with links to relevant SSAC documents/proceedings from the SSAC's website.

    Brief communications that can be shared within SO/ACs makes the SSAC more transparent and keeps SSR top of mind as an ICANN meeting approaches.

18. The SSAC should post specific additional materials online in the short-term, to consolidate information and increase transparency. The SSAC's Administrative Committee should then undertake a yearly review of the SSAC's website to determine whether additional content should be provided or whether the website should be restructured.

    Periodic website improvements increase transparency and can assist with member recruitment.

19. The SSAC should remain accountable directly to the ICANN Board and through it to the wider ICANN community.

    The current accountability mechanisms for the SSAC are appropriate.

Section VII relates to SSAC's size, membership, and term length and limits.

20. The current number of SSAC members is appropriate. The SSAC should continue to work to ensure its members are engaged, in conjunction with the recruiting points made below.

    There should be a yearly flow of individuals on to and off of the SSAC, providing new ideas and perspectives while retaining active members' expertise.

21. Each year, the SSAC should develop a formalized recruiting plan with goals, potential recruiting targets, meetings to attend, messaging for prospective candidates, and any other items that are deemed useful. Similarly, it should maintain a list of potential future members, even if those individuals are not currently applying to the SSAC.

    A formalized recruiting plan can help the SSAC to increase the robustness of its talent pipeline, ease the transition of retiring members, reflect on the required skills *and diversity for more medium-term goals, and grow its network in light of increased workload.*

22. The SSAC should work with the ICANN Board to secure funding to present its work at and/or attend two or three major security conferences outside of ICANN meetings annually, where members may meet new interested applicants.

    Both academic and professional conferences provide opportunities to meet established and emerging experts in SSR-related fields who could bring new and useful perspectives as future SSAC members or Invited Guests. It also can assist with increasing geographical diversity.

23. The SSAC Membership Committee should generate a list of academic or other institutions with research efforts in fields related to SSR. The Membership Committee should keep this list up to date, and consider if academics may bring useful perspectives as either Invited Guests or full SSAC members.

    Academics working in related fields may be interested in collaboration with the SSAC. A connection to academic institutions can also serve as a feeder for individuals to assist with SSAC work.

24. The SSAC should continue efforts to recruit individuals with a strong technical background but who also have legal/policy expertise. Discussion of the need for individuals with legal, policy, and law enforcement expertise should be codified in each year's recruiting plan.

    While the SSAC currently has members experienced in legal, policy, and law enforcement backgrounds, it is important that this continue to be a criteria that is considered when planning the SSAC's recruiting.

25. The SSAC should endeavor to recruit individuals with a strong technical background who also represent a broad set of geographical locations and reasonably balanced set of genders. Discussion of how to do so should be codified in each year's recruiting plan.

    When it is possible to obtain both diversity and the required technical expertise for the SSAC, processes should be in place that maximize the likelihood of doing so.

26. The SSAC's membership review process should include a yearly review process for the SSAC's external Liaisons and representatives.

    This informal review will provide feedback to the SSAC's external interfaces to help them identify actions that are seen as useful.

27. The SSAC's leadership should be limited to two, three-year terms. The SSAC should impose no term limits on non-leadership members.

    This aligns with the SSAC's current term limits, except for the SSAC Chair.

28. The SSAC should work with the ICANN Board to update the ICANN Bylaws in order to allow for there to be term limits on the SSAC Chair.

    After the update is made, the SSAC should term-limit its Chair as described above.

29. The SSAC should maintain its current processes and activities around disclosing potential conflicts of interest, both at the individual level and as a group of individuals. It should also update its online disclosure of interest statements to clearly articulate when the disclosure was last submitted for each member.

    In an organization such as the SSAC, it is impossible to assure a complete lack of conflict of interest on the part of each individual. Instead, the SSAC needs internal checks among the group of individuals to assure that conflicts are addressed and don't influence the institutional decisions of the organization.

Section VIII relates to the SSAC's prior review implementation and continuing efforts for self-improvement.

30. The SSAC should continue to nurture and build upon the SSAC's culture that values self-improvement, including between formal reviews.

    Effective organizations do not learn and improve only during formal processes, but via continuous reflection as experience is gathered. Such continual improvement allows an organization to learn in real time and to be robust to change.

Outside of these recommendations above, we note that in managing its work, the SSAC faces certain tensions. For example, while technical excellence is the foundation of the SSAC's credibility and excellence is strongly tied to the SSAC's consensus building processes, this can at times be in tension with the need to communicate more broadly and quickly to non-technical constituents. Similar tensions arise when balancing outside transparency into the topics discussed by the SSAC with the need for responsible disclosure that does not notify attackers of potential security risks, or when balancing organizational flexibility with the need to at times have well defined formal processes. Recommendations are made with the balance of these tensions in mind, as discussed further throughout this report.