ICANN

Review of the Security and Stability Advisory Committee

Draft Report

of the SSAC Review Working Group

September 2009

Table of contents

1. Background

As part of its program of Organizational Reviews, ICANN has undertaken a review of the Security and Stability Advisory Committee (SSAC), whose role[1] is to advise the ICANN community and Board on matters relating to the security and integrity of the Internet's naming and address allocation systems. This includes operational matters (e.g., matters pertaining to the correct and reliable operation of the root name system), administrative matters (e.g., matters pertaining to address allocation and Internet number assignment), and registration matters (e.g., matters pertaining to registry and registrar services such as WHOIS). SSAC engages in ongoing threat assessment and risk analysis of the Internet naming and address allocation services to understand where the principal threats to stability and security lie, and advises the ICANN community accordingly.

Organizational Reviews are part of ICANN's program of continuous improvement and are intended to ensure an in-depth examination of the role and operation of key structures of ICANN, with support from external, independent professional consultants.

As specified in Article IV, Section 4 of ICANN's Bylaws, the "goal of the review, to be undertaken pursuant to such criteria and standards as the Board shall direct, shall be to determine (i) whether that organization has a continuing purpose in the ICANN structure, and (ii) if so, whether any change in structure or operations is desirable to improve its effectiveness."

Oversight of the Organizational Review processes is exerted by the Structural Improvements Committee (hereinafter SIC), which is a standing Committee of the Board. The SIC is authorized to set up specific Working Groups (hereinafter, WG) for each of the Reviews.

With support from the ICANN Director for Organizational Review, the Review WGs have two main tasks:

- To ensure that the selected external reviewers carry out their task in full autonomy and independence of judgment, basing their conclusions and recommendations on evidence and in observance of the selected methodologies and workplan;

- After delivery of the reviewers' report, to carry out an extensive consultation with the community under review and any interested party on the conclusions of the external review, and formulate a report to the Structural Improvements Committee and the Board on measures to be adopted to increase effectiveness of the key structure under review.

---

[1] *As defined by Article XI, Section 2 of the Bylaws*

Chronology

In June 2008 the Board of ICANN approved the composition of a specific SSAC Review WG, which included the following individuals: Dennis Jennings (Chair, Board Member), Suzanne Woolf (Board Member), Robert Blokzijl and Reinhard Scholl (former Board Members). The WG was supported by Marco Lorenzoni, ICANN Director for Organizational Review.

Following an open selection procedure, in October 2008 the Board of ICANN appointed JAS Communications to undertake the independent, external review of the Security and Stability Advisory Committee (SSAC), and the selected consultants started their activities in November 2008.

In February 2009 the independent reviewers delivered their draft report, which was presented at the ICANN meeting in Mexico City; a 30-days public comment period followed, allowing reactions from the SSAC community and other interested parties. Following initial feedback and inputs from the WG, the reviewers finalized their [Final Report](), which was delivered in May 2009 and then posted for public comments.

In response to the Reviewers' reports, SSAC conducted a self-review exercise, which resulted in a coherent and comprehensive SSAC report to the Working Group, delivered in June, 2009.

The conclusions of this SSAC report were discussed with the SSAC Review WG at the ICANN Meeting in Sydney (June 2009), in order to better understand the different measures suggested by both the independent reviewers and the SSAC community.

This SSAC Review WG draft Report, will be posted for public comments and presented at the ICANN Meeting in Seoul before finalization.

The Members of the Working Group would like to express their sincere appreciation for the commitment and professionalism devoted to this review exercise by the external reviewers, JAS Communications, by the SSAC Chair, Steve Crocker, and by all SSAC Members involved in the self review exercise and coordinated by John Schnizlein.

Structure of the present report

The present report contains three sections, namely:

- Section 1 – the present Section, containing background information

- Section 2 – This section presents the conclusions of the WG on each of the Recommendations formulated by reviewers. Comments formulated by SSAC in their self review exercise are referenced, as well.

- Section 3 – WG conclusions on further SSAC proposals. This section presents the conclusions of the WG on further proposals formulated by SSAC and contained in their report 'SSAC review of SSAC'.

2. WG conclusions on independent reviewers' recommendations and SSAC comments

The Final Report of the independent reviewers contains 33 recommendations numbered from 1 to 33, and clustered in three different thematic groups:

- Organizational Clarity and Charter – recommendations from 1 to 14
- Formality and transparency – recommendations from 15 to 29
- Conflict of interest – recommendations from 30 to 33

The present Section presents a short summary of each recommendation issued by reviewers, and – per each of them – a comment synthesizing the respective opinion of the SSAC community and the conclusions of the WG (*in italics*). No comments are given for recommendations for which there is consensus, unless necessary.

Cluster	Organizational Clarity and Charter
Reviewers Recommendations	1. ICANN maintain an advisory body comprised of outside experts on the security and stability of the Internet's unique identifier systems. 2. SSAC maintain its fundamental identity as an Advisory Board chartered by and reporting to the Board of Directors. 3. As SSAC and RSSAC are designed for different purposes, we do not recommend the combination of these bodies. 4. SSAC members should not be required to sign confidentiality or duty of loyalty agreements with ICANN.
SSAC position	Agreement
WG conclusions	*Agreement*

Cluster	Organizational Clarity and Charter
Reviewers Recommendation	5. The SSAC Charter should be amended to exclude dealings with confidential or proprietary information absent specific guidance from the Board.
SSAC position	Disagreement Because SSAC is composed of security professionals who often deal with private information, this would unnecessarily hamper analysis by denying useful information.
WG conclusions	*The WG agrees with the comments formulated by SSAC and considers that there is no need to amend its Charter.* *It remarks that SSAC has a legitimate right to ask for access to confidential or proprietary information that is needed to fill its mandate, requests that need to be motivated by appropriate reasons.*

	However, this does not imply the right for SSAC to force ICANN – or any other party – to disclose any requested confidential or proprietary information. In case of its disclosure, this information has to be treated under the terms set/to be set by the owners of the information. In the case of requests to ICANN the WG suggests that the CEO, and if necessary the Board, should decide on the access to confidential or proprietary information, considering the reasons for the request, and the possibility to set and enforce specific terms of access.

Cluster	Organizational Clarity and Charter
Reviewers Recommendation	6. The SSAC Charter be amended to exclude involvement with or review of internal ICANN operations except as specifically directed by the Board.
SSAC position	Denying SSAC information about internal ICANN operations, including IANA functions, would unnecessarily hamper its analysis. Where contracts or normal employment practices (e.g. the name of an employee who made an error) prohibit disclosure, SSAC should not have special access, but review and access to information on operational function such as root system provisioning and root server operations, these functions should be within SSAC's purview.
WG conclusions	In the interest of ICANN, SSAC is entitled to signal to the ICANN Board and management whenever it considers that there are potential threats to the security and stability of the Internet caused by ICANN's internal operations. ICANN's internal operations, including IANA, should report to the Board after each security and stability incident and annually on the measures adopted to face threats to the security and stability of the Internet that may be caused by its internal operations. The Board will decide on the partial or full disclosure of these reports to SSAC, as appropriate.

Cluster	Organizational Clarity and Charter
Reviewers Recommendation	7. Correct the perception of SSAC "independence" through improvements in formality, transparency, and increased Board interaction without limiting SSAC members' freedom of expression (specific recommendations in multiple locations).
SSAC position	The independent objective analysis of SSAC is its greatest benefit to ICANN. Concerns that SSAC views its role as beyond advisory to the ICANN board stem from misunderstanding

	discussion of possibly responding to the root-signing NOI.
WG conclusions	*SSAC is committed to provide factual, evidence-based advice to the Board of ICANN, even if the Members of the Committee are not independent from their respective employing organizations. In this sense, the WG does not remark any contradiction between the status of several of the SSAC Members as employees of different organizations and the technical, analytic work that they perform for SSAC.* *The WG considers that no specific measures need to be adopted to address this remark, as other recommendations deal already with the same topic.*

Cluster	**Organizational Clarity and Charter**
Reviewers Recommendation	8. SSAC Charter be amended to add a requirement that the SSAC Chair and the SSAC Board Liaison are not the same individual.
SSAC position	We see no reason to either require or prohibit the same person from serving in both Chair and Liaison role.
WG conclusions	*The WG agrees with the comments made by SSAC, and does not consider that the SSAC Charter requires amendment in the sense suggested by reviewers.*

Cluster	**Organizational Clarity and Charter**
Reviewers Recommendation	9. ICANN reimburse travel expenses for the SSAC Chair to ICANN meetings when appropriate.
SSAC position	Agreement, with the remark that 'getting more SSAC members to ICANN meetings would help.'
WG conclusions	*The WG agrees with the recommendation of the external reviewers.*

Cluster	**Organizational Clarity and Charter**
Reviewers Recommendation	10. ICANN Board study the issue of paying a stipend or honorarium to SSAC Leadership and members.
SSAC position	Agreement
WG conclusions	*Agreement*

Cluster	**Organizational Clarity and Charter**
Reviewers Recommendation	11. The SSAC charter be amended to specifically include nontechnical risks to security and stability as within scope.
SSAC position	Although non-technical risks to security and stability are considered by SSAC, its focus should remain on objective facts

WG conclusions	*SSAC has already demonstrated being able to analyze technical consequences of non-technical decisions.*
	The WG considers that the SSAC Charter does not need to be amended in the sense suggested by reviewers.

Cluster	Organizational Clarity and Charter
Reviewers Recommendation	12. SSAC maintain focus on developing and sharing knowledge and understanding of new and evolving risks; SSAC should specifically avoid tactical involvement in response or mitigation activities.
SSAC position	Agreement; SSAC should avoid operational response and concentrate on systemic issues.
WG conclusions	*The WG agrees with both reviewers' remark and the response from SSAC; no specific actions are needed.*

Cluster	Organizational Clarity and Charter
Reviewers Recommendation	13. SSAC Leadership improve sensitivity to political and business issues by heeding the following advice: • Whenever possible, provide advance notice in the form of a professional "heads-up" when uncomfortable situations are reasonably foreseeable. Avoid the perception of "blindsiding" individuals and entities. • Recognize that as an advisory body, SSAC's role is to provide the best advice possible. There is however no requirement for anyone to follow SSAC's advice. • Recognize that ICANN has complex business relationships with many of the same entities SSAC may be issuing recommendations to. At times SSAC guidance may be in conflict with contractual obligations. • SSAC is a very visible and well-respected brand. SSAC is closely watched globally and people pay attention to what SSAC says. To maintain the value of SSAC's brand, SSAC must continue to conduct itself with the highest level of professionalism and integrity.
SSAC position	Agreement. The detailed advice does not actually impinge on SSAC's goal of objectivity as long as it is limited to (1) avoid blindsiding individuals, (2) recognition that there is no requirement for anyone to follow SSAC's advice, (3) SSAC's guidance may conflict with contractual obligations, and (4) SSAC must continue to conduct itself with the highest level of professionalism and integrity.
WG conclusions	*The WG agrees with the comment formulated by SSAC, and*

considers that no action is required.

Cluster	Organizational Clarity and Charter
Reviewers Recommendation	14. The SSAC charter be amended giving guidance to focus on issues of strategic and policy importance and to avoid tactical operational issues except as charged by the Board.
SSAC position	The current charter adequately indicates that SSAC's mission is strategic rather than operational.
WG conclusions	*The WG agrees with the comment formulated by SSAC, and considers that no action is required.*

Cluster	Formality and Transparency
Reviewers Recommendation	15. In conjunction with the ICANN Board, staff, and public consultation, SSAC undertake an annual planning process to review the previous year and determine the research and publication agenda, membership strategy, and resource requirements for the coming year. The annual plan will be presented to the Board for approval.
SSAC position	Although a planning process is necessary, it should not be constrained to annual cycles. The budget to accomplish the plan should be presented for Board approval.
WG conclusions	*The WG agrees on the need for SSAC to setup a lightweight planning process.*

Cluster	Formality and Transparency
Reviewers Recommendation	16. SSAC keep and publish meeting minutes on the SSAC web site in a timely fashion.
SSAC position	Agreement, with the understanding that minutes are not the same as transcripts
WG conclusions	*The WG agrees with both reviewers' remark and the response from SSAC.*

Cluster	Formality and Transparency
Reviewers Recommendation	17. SSAC should endeavor to keep their web site current to include work in progress and work planned for the future.
SSAC position	Agreement; SSAC's web site requires constant maintenance.
WG conclusions	*Agreement.*

Cluster	Formality and Transparency
Reviewers	18. As a part of SSAC's first annual plan, SSAC revisit task area

Recommendation	one in conjunction with ICANN staff. Task area one reads as follows: "Develop a security framework for Internet naming and address allocation services that defines the key focus areas, and identifies where the responsibilities for each area lie."
SSAC position	The first item in the current charter (…) should be removed.
WG conclusions	*Agreement with the proposal formulated by SSAC.*

Cluster	**Formality and Transparency**
Reviewers Recommendation	19. SSAC should endeavor to find the best experts globally without regard for geographic proximity. SSAC membership should not be subject to artificial geographic quotas. 20. SSAC membership appointments be for a term of three years, renewable by the Board at the recommendation of the SSAC Chair indefinitely. 21. Do not impose a limit on the number of terms an SSAC member may serve. 22. Stagger SSAC member terms such that roughly 1/3 of the terms are up for renewal each year.
SSAC position	Agreement
WG conclusions	*Agreement*

Cluster	**Formality and Transparency**
Reviewers Recommendation	23. SSAC Board Liaison be permitted a maximum of three consecutive one-year terms.
SSAC position	Disagreement
WG conclusions	*The WG considers that all Liaisons should be appointed for a three-year term, with the possibility to serve for a maximum of three consecutive terms.*

Cluster	**Formality and Transparency**
Reviewers Recommendation	24. Article XI of the ICANN Bylaws be amended to include a new section discussing the removal of an advisory committee member or chair through a simple majority vote of the Board.
SSAC position	The combination of constraints on membership of (1) approval if individual members to (2) three-year terms, with (3) renewal dependent on peer review is adequate. Any appearance that the board can punish a member of SSAC for leading an unpopular study would undermine credibility.
WG conclusions	*The WG agrees that protective measures should be put in place to remove disruptive or underperforming AC Members or Chair.*

Cluster	Formality and Transparency
Reviewers Recommendation	25. SSAC implement a policy explicitly stating that the SSAC brand (written or verbal) is to be used only on approved work products.
SSAC position	The focus on "branding" is inconsistent with the objective fact-based approach that is SSAC's primary distinctive value.
WG conclusions	*The WG considers that – if and when applicable – when making statements SSAC members should clarify whether they refer to their personal view or to positions expressed in SSAC documents.*

Cluster	Formality and Transparency
Reviewers Recommendation	26. The SSAC Chair select, implement, and enforce the regular use of a transparent decision making and documentation strategy fitting of the membership and culture of the SSAC.
SSAC position	The formality of quorum, voting, Robert's Rules, recusal, dissent and approval are unnecessary because SSAC is not representational.
WG conclusions	*The WG agrees with the recommendation issued by reviewers and remarks that the position of SSAC was formulated in response to the initial draft version of reviewers' report, which contained an excessively formal approach to document decision making and documentation processes. The final version of reviewers' report formulates proposals that appear consistent with the culture of SSAC.*

Cluster	Formality and Transparency
Reviewers Recommendation	27. The SSAC formally approve and release all work products pursuant to the chosen decision making and documentation strategy.
SSAC position	Disagreement, same motivation as above (Rec. 26)
WG conclusions	*Same comments formulated in relation to Recommendation 26.*

Cluster	Formality and Transparency
Reviewers Recommendation	28. SSAC formally and visibly adopt a suitable default confidentiality policy. Other policies are used as necessary by mutual agreement.
SSAC position	Agreement
WG conclusions	*Agreement*

Cluster	Formality and Transparency

Reviewers Recommendation	29. Utilize the mechanisms recommended in this review, including the annual planning process, to regularly evaluate SSAC performance against objectives and resource utilization.
SSAC position	Disagreement; evaluating performance against objectives is appropriate for employees, but not for volunteer experts often from outside the domain-name business.
WG conclusions	*The WG recommends that SSAC produces a lightweight, yearly report of activities to the Board; the report should be published as appropriate.*

Cluster	Conflicts of Interest
Reviewers Recommendation	30. SSAC publish simple conflict disclosure forms for each SSAC member on its web site. Candidate SSAC members will be required to provide a complete disclosure to the Board prior to appointment to SSAC, and shall provide an updated disclosure whenever circumstances merit.
SSAC position	We agree conflicts of interest should be disclosed, but prefer not to use formal, signed statements and keep these disclosures less formal.
WG conclusions	*Agreement with the recommendation formulated by reviewers and the approach proposed by SSAC.*

Cluster	Conflicts of Interest
Reviewers Recommendation	31. Each SSAC work product shall include a "Dissents" section. Any SSAC member wishing to dissent shall do so here by name or anonymously. If there are no dissents, the verbiage "No Dissents" shall appear. 32. Each SSAC work product shall include a "Recusals" section. The name of any SSAC member who recused him or herself during any part of the preparation and discussion of the specific work product shall appear here. If the individual wishes to remain anonymous, the term "X Recusals" shall appear in this section, where X is the number of anonymous recusals. If there are no recusals, the verbiage "No Recusals" shall appear. 33. SSAC develop and post a conflicts of interest policy based on the ICANN Board policy.
SSAC position	Agreement
WG conclusions	*Agreement*

3. WG conclusions on further SSAC proposals

The report issued to the SSAC review WG from the SSAC community contained nine further recommendations that did not make direct reference to recommendations issued by external reviewers; they are reported in the present section, together with the conclusions of the Working Group.

For ease of reference, they are numbered from 1 to 9.

SSAC recommendation	1. The SSAC Charter should be reconsidered as part of the regular review process
WG conclusion	*The WG agrees and remarks that the standard Terms of Reference of each organizational review of the key structures of ICANN already include this point of analysis.*

SSAC recommendation	2. A membership committee should review individual contributions regarding renewal of terms
WG conclusion	*The WG agrees with this proposal, which is an operational measure aimed to implement the reviewers' recommendations 20 and 21.*

SSAC recommendation	3. SSAC should (continue to) choose what studies to pursue
WG conclusion	*SSAC should continue to choose the studies it pursues, being sensitive to the concerns of and issues identified by ICANN's stakeholder community. The ICANN Board may also task the SSAC.*

SSAC recommendation	4. SSAC should consider which reports to ask ICANN to translate into other languages
WG conclusion	*The WG agrees with this proposal.*

SSAC recommendation	5. SSAC should consider (staffing) a continuing process of feedback from the ICANN community on its work
WG conclusion	*The WG agrees with this proposal.*

SSAC recommendation	6. SSAC should conduct a dedicated meeting annually
WG conclusion	*The WG sees merit in SSAC developing such a proposal to ICANN*

SSAC recommendation	7. ICANN's regional liaisons should provide periodic briefings to SSAC members
WG conclusion	*The WG agrees in principle with this proposal; the professional profile of the regional liaisons shall be taken into account when defining the content of these briefings.*

SSAC recommendation	8. SSAC should consider maintaining public comments on its documents
WG conclusion	*The WG agrees in principle with this proposal, but SSAC should not introduce public comment periods that delay the delivery of SSAC reports.*

SSAC recommendation	9. Executive Committee minutes should be made available to SSAC members
WG conclusion	*The WG agrees that SSAC Executive Committee minutes should be made available to SSAC members.*