SAC 39
SSAC Review of SSAC

A Report from the ICANN
Security and Stability
Advisory Committee
(SSAC)
15 October 2009

Preface

This is a report by the Security and Stability Advisory Committee (SSAC) that details the findings of the SSAC internal review of SSAC. The SSAC advises 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 assess where the principal threats to stability and security lie, and advises the ICANN community accordingly. The SSAC has no official authority to regulate, enforce or adjudicate. Those functions belong to others, and the advice offered here should be evaluated on its merits.

The contributors to this report, reference to the committee members' biographies and statements of interest, and committee members' objections to the findings or recommendations in this report, are at end of this report.

Table of Contents

Appendices

Introduction

The SSAC bylaws require a periodic review of each component of SSAC, including each supporting organization (SO) and Advisory Committee (AC). The ICANN Board initiated the review of SSAC in June 2008, which included an external review by JAS Communications. (See SSAC Review: Independent Consultants' Report.)

In addition to participating actively in the external review, we have also taken the opportunity to gather our own thoughts on what we're doing, whether we're doing the right things, and how well we're doing them. We carefully chose to initiate this process after the external review was completed in order not to bias the external review. We report here the results of our internal review.

The periodic external review of ICANN Advisory Committees does not preclude, and provides prompting for, review of SSAC by itself. This review is organized around what we regard as the essential questions, two of which are existential, the rest of which are matters of implementation.

Existential questions

Whether ICANN needs SSAC, and what SSAC should do, are essentially questions that only the ICANN Board can answer. We only provide advice on what should be considered.

1. Does ICANN Need SSAC?

That SSAC has a history of accomplishment (see Appendix 1 and 2) is insufficient for answering this question. Just because SSAC has been productive does not imply that it should be continued. However, SSAC's past productivity suggests that its members have the necessary competence and independence, and that this will guide its selection of members (see section 3), with board approval as the guarantor that the Chair selects members fairly.

Unlike the Supporting Organizations and the other Advisory Committees, SSAC does not represent a constituency and has no formal role in the operation of ICANN. Instead, SSAC provides objective analysis based on facts by technical experts. ICANN needs to ensure that a compromise among competing constituencies does not lead to policy that is technically infeasible or unsafe. If the ICANN board did not have this independent, external source of advice, it would be necessary to create it or something else to replace it.

Several alternative structures deserve to be considered.

1. A standing committee, as SSAC is currently structured, has the advantage of

assembling a sufficiently broad set of experts over time before they are needed, avoiding delay and potential risk of not finding willing expertise when an issue arises. A standing committee also provides a good source for identifying issues. But the difficulty of getting work from a standing committee of volunteers is a constant problem for SSAC.

2. Professional staff with the mission of strategic analysis now assigned to SSAC would solve the commitment problem, but it is likely difficult to keep them separate from operational demands.

3. Paying consultants for individual studies runs the risk that they provide the answer they think you want in order to obtain future business.

4. The RTSEP process of maintaining a pool of experts from which working groups are formed for individual studies may be an effective hybrid of the other structures. Paying working-group members would solve commitment problems, but would then exclude the experts who are full-time employees of other organizations.

5. A different hybrid approach of adding professional staff while improving the engagement of standing committee members is worth trying

But SSAC's opinion that its existence and function is necessary is not the critical question. It is essential that the ICANN board see the value as high enough to qualify as "necessary" for independent technical fact checking. If ICANN really needs SSAC, it will not restrict SSAC's scope, as considered in the next question, because without access to facts and unencumbered technical advice, its analysis would be hampered. From a broader perspective, with the creation of other security activities within ICANN, it's important for the board to clarify the role and necessity for SSAC.

2. What Should SSAC Do?

The SSAC charter (Appendix 3) should define the scope of SSAC's activity. This charter should be reconsidered as part of the regular review process.

As a creature of the ICANN Board, SSAC serves the Board with unbiased external advice. Because of ICANN's multi-stakeholder mission, SSAC must also advise ICANN's constituencies. Responsibility to both is explicit in the charter. This responsibility is not so broad as to cover security and stability of the whole Internet, however; it is limited to the security and stability of the Internet's unique sets of names and numbers. Other items in the charter elaborate on specific responsibilities beyond advising the board.

The first bullet in the current charter, "To develop a security framework for Internet naming and address allocation services …" is more appropriate for research and development than for an advisory committee composed of volunteers. SSAC has not attempted such a framework, and there is little reason to think it will. This item should be removed from the charter. ICANN should consider requesting this sort of effort from the Internet Research Task Force.

The second bullet of the charter calls for SSAC interaction with the Internet technical community and managers and operators of critical DNS infrastructure. Any reasonable interpretation of this would include operations such as the IANA (Internet Assigned Number Authority) function for names and addresses. IANA has a critical role, and works closely with the IETF (Internet Engineering Task Force). There are reasons to exclude IANA functions from SSAC study, but except where those reasons exist, IANA functions should be open to SSAC. Certain information cannot be shared publicly, for various reasons. If such information is necessary for SSAC to perform its functions, SSAC members can sign nondisclosure agreements as appropriate. This charter item should not be changed. However, care should be taken that SSAC is not burdened with operational tasks or steps onto the turf of other groups (standard audits, RSSAC etc.). The clearest line between what should and should not be within SSAC's purview is that SSAC studies systemic issues rather than responding to individual incidents.

For effective analysis, SSAC needs complete access into core information about security-relevant processes, whether inside or outside ICANN. If there are aspects that require care (secrecy) in handling, appropriate arrangements can be made.

Implementation Questions

The following questions regard how SSAC should operate, and are more reasonably matters for SSAC determination. These questions, from membership, through process and projects, to transparency and resource requirements, have been raised either in the external review process or by members. We treat this review as an opportunity to more directly design SSAC's operation, which has largely evolved up until now (see Appendix 1).

3. How Should Membership Be Determined?

SSAC members are volunteers invited by the chair as recognized experts in some area(s) of Internet security and stability. It is common for an individual to participate as an invited guest for some time before his or name is presented to the ICANN Board for formal appointment to SSAC. An effort is made to include individuals with a wide variety of backgrounds. There are no limitations on the term of a SSAC member. In addition to having prospective members as invited guests, the same procedure is sometimes used to bring people into a specific project.

Another perspective on this question is why would anybody want to be on SSAC? The dominant motivation is that people care about the security and stability of the Internet, and want to give ICANN their best advice on how what ICANN does can preserve and extend it. Members' concerns about trends and events motivate their participation in SSAC projects where there is a subset of SSAC members qualified on a subject. The number and variety of SSAC projects is noteworthy considering how voluntary participation is. Membership is about doing the work because there is no other reward and very little status.

As part of clarifying SSAC membership, the fluid membership status should be replaced with renewable three-year terms. The expectation that significant contribution to a relevant subset of SSAC's studies needs to be clear to candidates.

It would be useful to provide some data on the kind of characteristics, affiliations and traits we are looking for in SSAC members. In some ways, we are running a constant "nominating" process, and we ought to codify the characteristics we hold dear so there is a lesser chance of erosion as time passes.

One of the advantages of a three-year term is that members do not all contribute equally (or at all) on several topics. They tend to self-select on the topics that matter to them, and such topics might only come up once in 10 or 15 months' time. Annual reviews of contribution to SSAC, and value from SSAC should also be conducted. A membership committee could be maintained, with rotating membership, would advise the Chair on member recruitment and retention. Limiting the size of SSAC would interfere with it retention and recruitment of the widest variety of experts.

4. Should SSAC Adopt Formal Processes?

The current process of open and fact-based discussion of facts and analysis led by the most expert subset of SSAC membership works well because SSAC does not represent constituencies, unlike most of the other ICANN committees. Where different constituencies are represented, formality can mitigate conflict during negotiations, but it is an unnecessary burden where objective analysis that every competent member can see leads to consensus. Where analysis does not produce consensus, SSAC strives to objectively describe the alternatives.

As in the IETF, voting is irrelevant to finding the best objective outcome. SSAC seeks consensus, obviating dissenting or minority reports. Without voting, there is no need for a quorum for each meeting. Without any need for a quorum, there is no need to limit the number of members or the frequency of meetings. Without representation and voting, there is no need for a formal process such as Roberts Rules[1] to ensure each position gets a fair opportunity to be heard.

---

[1] Roberts Rules: http://en.wikipedia.org/wiki/Roberts_Rules

Abstention and dissent are available (possibly not clearly enough) within SSAC now, and should remain, although they are also more associated with representation of different positions than science. Abstention should be reserved for matters of professional ethics because it is often the person with direct involvement in a matter who is most knowledgeable. If we make a practice of excluding people who are closely involved, we probably deprive ourselves of the best information available. Formal recusal in deference to other members with greater expertise in the topic at hand would be a waste compared to the current practice where members speak up only when they have expertise to offer. The normal process should be that SSAC documents will contain clear statements regarding dissent.

Because SSAC advises, rather than makes policy, dissent would usually take the form of describing multiple analyses, conclusions, or perspectives, preferably with the different conditions leading to each.

The process of completing a project or report could use more formality so that those less directly involved know when a final reality check from different perspectives is called for. A last-call process, as used in the IETF, works better in SSAC, where eleventh-hour objections are accommodated, than votes of approval would.

5. How Should Individual Studies Be Selected?

SSAC should continue to determine what studies, projects and reports to pursue. SSAC should publish the criteria that determined adoption of each project.

In cases where an Supporting Organization requests SSAC to do work, or the Board requests us to study an important topic, SSAC needs to create a repeatable process that takes us step-by-step through creating terms of reference, study plan, steering committee, etc., as necessary.

The ideas of formal tasking by the board and annual project planning are too unresponsive to concerns that emerge in the Internet. It is in the nature of security and stability that they are often best detected in their absence. An ongoing open process as described above would be more responsive and accountable than a rigid annual list from the Board. Annual planning (see section 8) would take the pattern of project approvals into consideration.

6. Should SSAC Have Additional Roles and Structure?

Yes, SSAC should establish regular process and assignments for a Membership committee. (See section 3.) While not really new, the role and structure of SSAC's Executive Committee (ExecCom) should be better documented. Structure should be added only slowly and carefully to preserve the collegial operation of SSAC.

SSAC should better define and map out all roles: Chair, Vice Chair, Board Liaison, Secretary, Fellow (or equivalent title), Member, Invited Guest. We should add job definitions. We should adequately document the amount of time required for SSAC work, what kind of inputs and outputs are expected for each role, and subject these to periodic review. Candidates for these positions must enter them with a clear understanding of what they are signing up to, and what they can expect to contribute as well as to learn from their involvement. Liaisons from other parts of ICANN are welcome, but must meet the requirements of SSAC and become full members.

In addition to the ExCom and the Membership sub-committee, SSAC should consider a standing subcommittee on the review of SSAC, which is too big a task to just add to the ExCom. Continuous self-review would serve to reinforce the essential objective analysis that characterizes SSAC. SSAC should also maintain a membership committee, as suggested in section 3.

7. How Could SSAC Improve Transparency in its Operation?

SSAC has performed largely on its own, without clear exchange of information with the rest of ICANN. There are a number of opportunities to improve the transparency of SSAC's operation without interfering with the discussion of sensitive information.

Several improvements are implied by discussion above:

- SSAC should better keep timely public records of its membership.
- The process of the ExCom should be published to the ICANN community.
- SSAC should publish the criteria that determined adoption of each project. (See section 5.)
- SSAC should keep better records informing the Board and the ICANN community what studies and projects it has underway or under consideration. (See section 5.)
- SSAC structure and roles should be better documented for the ICANN community. (See section 6.)

SSAC should make its work available in the various media forms that are available to it. For instance, if videos of presentations are available, they should be uploaded to the SSAC site. Edited video or excerpts might be suitable for mediums such as YouTube, which make the SSAC output more accessible that posting solely on the ICANN website.

SSAC began translating documents in mid-2008 but to date, has been selective in choosing which documents to translate. ICANN has streamlined its translation processing. SSAC has begun making use of the same submission process in preparation for the Sydney meeting and will attempt to make publications available (nominally in the official UN languages) in a timely fashion following their initial publications in English.

SSAC's way of soliciting feedback on its work product is somewhat ad-hoc. A more structured approach would require a staff function whose primarily role is to engage with other constituencies and communities to solicit feedback and to provide input on our tasks and documents.

Transparency is not just about documentation, but also the sense that SSAC is part of the ICANN community, which would be improved by SSAC members attending ICANN meetings. SSAC members who attend an ICANN meeting should be provided an orientation to the meeting, included invited talks by various constituencies so the members get a sense of the breadth and depth of issues that are important to the community SSAC serves. Recognizing that many SSAC members are time constrained, SSAC members should be afforded the opportunity to attend at least one ICANN meeting a year, with travel & lodging expenses borne by ICANN. Travel & Lodging support should be a line item in the SSAC budget request to the Board and should adhere to regular ICANN travel and expense policies.

8. How Could SSAC Be More Effective?

Internal discussions have suggested several ways in which SSAC can make its internal operation more effective.

SSAC Liaison: The Liaison role involves essentially full participation on the ICANN Board and hence is a fair amount of work. If the SSAC Chair also serves as the Liaison, the person should be able and willing to assume both roles. We see no reason to either require or prohibit the same person from serving in both roles.

Dedicated Meeting: SSAC should conduct an annual retreat with a defined agenda and ability to discuss organizational, political, process or other substantive issues not normally amenable to discussion lists and telephone conferences. It is likely that the list of topics covered change from year to year, but some core topics such as organization and policy will persist.

Annual Planning: SSAC, as part of its annual planning process, needs to develop a list of strategic priorities for the succeeding year (and subject it to the normal internal and external review process). Each of these priorities needs to be explained in broad-brush projects, which have targeted amounts of time, money and staffing scoped. This annual planning process is not intended to preclude projects being adopted more quickly as described in section 5.

Budget Request: Once this is complete, the outcomes should be compiled into a budget request that is added as part of the normal ICANN budgetary process. This requires SSAC members on the Board to liaison closely with the Board Finance Committee, as well as with ICANN Finance staff. The SSAC Chair and Board Liaison will need to report back periodically to SSAC members regarding progress on this item.

Regional Interaction: ICANN periodically holds regional meetings. In addition, most regions of the world are now being covered by ICANN staff (regional liaisons). One of the roles of these liaisons should be to provide periodic briefings about the activities that ICANN is participating in to SSAC members in the region.

Web site: The SSAC web site would benefit from more timely maintenance and administrative updates. There are two components to this task: (a) regular maintenance and administrative updates to the web site, and (b) addition of news items, press pickups, highlighting of key reports made by SSAC. SSAC members should pay more attention to the web site, identify shortcomings, provide information to support staff they would like to see on the web site. A website update should be included as part of 2010's budget request.

Public Comments Archive: We have discussed instituting a process where each document is placed for public comment, and upon comments being received, the documented appropriately amended. The final document should be the only document on the main page – drafts, and comments should be placed on a separate archive section.

Minutes: SSAC minutes are maintained at the committee Wiki, as are SSAC ExecCom minutes. SSAC's philosophy is that premature disclosure of information during an information gathering stage or sharing of information made available in confidence with SSAC could hamper or compromise studies and thus minutes are not publicly accessible because they typically contain sensitive information.

9. What Resources Should SSAC Have?

SSAC members conduct committee business through mailing list participation. SSAC has a standing time slot reserved for weekly teleconferences. Teleconferences are canceled when the committee has no urgent business to conduct. The time slot is fixed and is intended to allow most members to participate at a reasonable time in their local time zone. The committee could consider rotating teleconference time to allow all members to participate at least once per month during reasonable (business) hours. SSAC has just one ICANN Senior Security Technologist, Dave Piscitello, and executive support from Julie Hedlund. The SSAC Chair, SSAC Liaison to the Board, Dave and Julie meet as an ExCom weekly to track progress and determine the need and agenda for the conference call. The identified leader of each project is invited to report progress at these executive committee calls. SSAC holds face-to-face meetings opportunistically at scheduled ICANN and IETF meetings, which are attended by varying subsets of the membership.

ICANN should provide the resources implied by the budget process described above, including travel and accommodation for SSAC members attending ICANN meetings.

Staffing resources are necessary to address several of the improvements identified above. We need multiple writers who have, among them, the breadth to cover the full range of SSAC issues, including domain name protection, root operations, IDN details, etc. In addition to the technical professional staff (like Dave), SSAC needs the sort of support staff that Supporting Organizations and other Advisory Committees have. Attempting to mix these different staff functions interferes with both. We need staff to help us engage substantively with other parts of ICANN, including understanding the policy development process and other procedures and fitting our work into the work of the staff, the SOs and the other ACs. We need to maintain our portion of the web site, provide useful summaries, and reach out through multiple channels, etc., i.e. the public relations aspect of our work. We need to follow up on what we've done in the past to measure our effectiveness. We need logistics support for the committee -- agenda, phone calls, minutes, etc.

Acknowledgments, Statements of Interests, and Objections and Withdrawals

In the interest of greater transparency, we have added these sections to our documents to provide the reader information on three aspects of our process. The Acknowledgments section lists the members who contributed to this particular document. The Biographies and Statements of Interest section points to the biographies of the Committee members and any conflicts of interest, real, apparent or potential, that may bear on the material in this document. The Objections and Withdrawals section provides a place for individual members to disagree with the content of this document or the process for preparing it.

Acknowledgments

The committee wishes to thank the following members for their time, contributions, and review during SSAC's study of this matter:

Jaap Akkerhuis
Steve Crocker
Jim Gavin
Warren Kumari
Dave Piscitello
Ram Mohan
Danny McPherson
John Schnizlein

Statements of Interest

SSAC member biographical information and Statements of Interest are available at:
http://www.icann.org/en/committees/security/biographies.htm.

Objections and Withdrawals

KC Claffy and Steve Crocker asked that their statements be included.

Statement of KC Claffy

[I should note that the JAS recommendation to have written dissents to SSAC reports was one I questioned in my comments on the first draft of the JAS report (16 feb 2009). Illustrating my concerns, only 6 of the 27 listed SSAC members indicated they had read this report (Jaap, Matt, Danny, Mike, Dave, Steve, and I), and all of them but Steve had

substantive problems with the report. [2] No one ever said they supported publishing this draft as is. But as requested I reluctantly submit this dissent.]

My biggest concern with this report is the process -- SSAC did not give JAS a chance to incorporate any formal SSAC comments to their report, though there was a two-month comment period explicitly intended for this purpose. Instead we intentionally attempted to re-frame the conversation by writing our own report to portray the committee better. This strategy was based on a private conversations Steve had with ICANN board members who approved it. This is not transparency of process.

I also reported about a dozen technical issues with SSAC's self-assessment, including that our responses to various JAS recommendations (15,29) contradict themselves, each other, and the text in the report. Our self-assessment report also dismisses some of their recommendations (7,18,23,25) with unrelated or false counter-claims, even for recommendations we are already trying to follow (26,27,29,30). My last round of comments on the self-assessment received no response from anyone on the list, though I later found out a few of my comments were integrated silently without mention or changing its date/version. This is not transparency of process nor is it coherency of position.

Statement of Steve Crocker

As noted in the introduction, this review was purposely initiated after the JAS review was complete. This decision was mine. I felt it would be inappropriate to do our own review before or during the JAS review because it would give the appearance of trying to control the outcome of their review. During the JAS review, many SSAC members interacted with JAS, often multiple times and at length. I am confident JAS had ample opportunity to hear a range of views from SSAC members and their recommendations reflected their judgments. I accept sole responsibility for choosing to have a separate internal review and for scheduling it after the external review was complete.

---

[2] SSAC Members and Invited Guests at the time the report was drafted were: SSAC Members: Alain Aina, Jaap Akkerhuis, Jeffrey Bedser, Lyman Chapin, KC Claffy, Steve Crocker, Patrik Fältström, Rodney Joffe, Olaf M. Kolkman, Mark Kosters, Matt Larson, Danny McPherson, Ram Mohan, Russ Mundy, Frederico A C Neves, Dave Piscitello, Ray Plzak, Ramaraj Rajashekhar, Barbara Roseman, Shinta Sato, Mark Seiden, Doron Shikmoni, Mike St Johns, Bruce Tonkin, Paul A Vixie, Suzanne Woolf, Rick Wesson; Invited Guests: Harald Alvestrand, Roy Arends, Steve Conte, Robert Guerra, Duncan Hart, Jeremy Hitchcock, Warren Kumari, Douglas Maughan, Christophe Reverd, John Schnizlein, Dan Simon, Stefano Trumpy, Patrick Vande Walle, Richard Wilhelm.

Appendix 1: SSAC History

[This appendix was written by Steve Crocker, SSAC Chair]

SSAC was activated in early 2002. It was formed in the aftermath of 9/11, a period when every organization asked itself what it should be doing about security. ICANN held a symposium on security in Marina del Rey in November 2001. The report from that symposium is reprinted as SAC 002.[3] The decision to form SSAC apparently followed that meeting. In short order, members were recruited, a charter drafted and the Committee was started. I was recruited to chair the Committee after its members had been recruited, and we began organized discussions in early 2002.

Our first discussions centered on DNS configuration issues, e.g. how many DNS operations were broken and to what degree? We also began discussion of DNSSEC.

Our early discussions were ad hoc, and we lacked any formal support. After a while, I asked ICANN to support an executive director and I recruited Jim Galvin. By mid 2003 we were holding regular calls and eking out reports. In September 2003, VeriSign released its SiteFinder service. SSAC quickly was actively involved in discussions and meetings, with two public meetings in October 2003 that included multiple presentations and full transcripts. However, preparation of a formal report exceeded our capacity for several months. We eventually got support to hire a writer, Amy Friedlander, and produced SAC 006,[4] "Redirection in the COM and NET Domains," 9 July 2004.

Taking a lesson from that experience, we created the position of "SSAC Fellow" and recruited Dave Piscitello to be a paid staff person to write technical reports on behalf of the Committee. The original plan was to bring in a senior person for a year or so, more or less along the lines of the fellowships sponsored by the IEEE[5] and other organizations to bring technically qualified people to work in various parts of the U.S. government for a year or so. Dave worked out spectacularly well, and we dispensed with the idea of forcing a rotation every year. (Indeed, the term "Fellow" turns out to be ambiguous, as it is also used in a much different senses, including ICANN Fellows who are provided travel support for participation in ICANN meetings.[6])

Since then, our production of documents has increased measurably. From our inception through 2005 we had produced seven reports. In 2006, we produced eight reports, more than doubling our lifetime total. We produced another eight in 2007 and a full dozen in 2008.

---

[3] http://www.icann.org/en/committees/security/sac002.htm
[4] http://www.icann.org/committees/security/ssac-report-09jul04.pdf
[5] http://www.ieeeusa.org/policy/GOVFEL/state.asp
[6] http://www.icann.org/en/fellowships/

SSAC Review of SSAC

When SSAC was first in operation, we had conference calls once a week. Participation was variable. Some members participated regularly; others only rarely. After a while, I started to have weekly calls with Jim, Dave and Ray Plzak who had volunteered to become vice chair, and we used these calls to organize and pursue the agenda for the Committee. Our weekly calls with the whole Committee became a bit intermittent, and we revised our schedule to have monthly calls as needed, with each call focused on a specific topic and planned in advance.

The level of participation has continued to be a concern. Dave's yeoman efforts preparing reports has perhaps engendered a relaxed posture from much of the rest of the Committee. In principle, our Reports, Comments and Advisories reflect the consensus of the Committee. In practice, only a small fraction of the Committee is actively involved in each effort. One of the questions for us to consider is whether this is a problem, a positive feature, or just an incidental fact. From my point of view, it's necessary to get others to take leadership roles in our projects and we started forming small working teams, each with a designated leader and named participants. As I write this, I have to say we don't have enough data know whether this will work. More on this below.

Another piece of our history relates to DNSSEC. In our early days, we spent much of time discussing and promoting DNSSEC. Bruce Tonkin took me aside during the Tunis meeting in October 2003 and pointed out that our DNSSEC efforts were underpowered. He suggested there needed to be separate funding and put on its own track. I began exploring that possibility, and, rather fortuitously, the newly formed cyber security program within the recently formed U.S. Department of Homeland Security included DNSSEC as part of its initial portfolio. At the same time, the Swedish registry, .SE, pushed forward with its very substantial effort to support DNSSEC, and multiple other implementation efforts took place, particularly at NLnet Labs and Internet Systems Consortium. Within the ICANN arena, we initiated a separate track of DNSSEC "workshops" – these were really "sessions" or "symposia" – at each ICANN meeting which provided a forum for publicizing progress, bringing people together who were working on DNSSEC, and raising awareness across the ICANN community. The DNSSEC effort involves too many people and too many organizations for SSAC to take sole credit for the progress to date, but I think our efforts have helped the cause.

Looking at our history from a different dimension, it's useful to see what topics we have dealt with and where they fit into the larger picture. We have designated our documents as Reports, Advisories and Comments. Reports are our primary output, usually representing a few to several months of effort. Advisories are much shorter term efforts intended to give advice quickly. We're not organized to do this very well, so we don't have very many. Comments are responses to other documents, often but not exclusively ICANN planning documents. I went through our 38 documents to date, including three for 2009, one of which is not yet published but which is far enough along to include,[7] and I assigned each to a "Topic." These assignments are my own and not necessarily the

---

[7]SAC 037 will be a report on IDN and Whois. For categorization purposes, I put it under the IDN topic, though it also applies to Whois.

same as anyone else's, and they're definitely not official. Nonetheless, they give a useful picture of where we've spent our time and attention. Of our 38 documents, eight address various issues of registration abuse and five more are focused on whois issues. The next highest topics are Redirection and DNSSEC, with four and three documents respectively. We also have three documents focused on IPv6 and root, and another two focused on just IPv6. The rest are spread thinly across other topics.

When we started, I had guessed we would be focused primarily on core DNS operational issues, e.g. configurations, lame delegations, deployment of DNSSEC. Instead, registration issues, e.g. hijacking, unintended consequences of released registration, whois listings, etc., have been our most common focus. Even though we gave extraordinary attention to the redirection issue (SiteFinder) in 2003, only occasionally did it reappear, and we have issued only four documents in total on this topic.

ICANN's History

Over this same period of time, ICANN has evolved and changed considerably. I won't try to give a balanced picture of all of ICANN's activities. Instead, here's a brief compendium of major events and changes that intersect our interests. (I suspect this is not complete. I apologize if I have left out anything.)

From 2002 to 2009:

- ICANN has evolved from a 3½ year old organization to a 10½ year old organization. ICANN is now 3 times as old as it was when it started, and hence SSAC has been part of ICANN for 2/3 of its lifetime.

- ICANN's budget has grown from a few million dollars per year, which was just barely enough to keep it alive, to more than $60 million annually.

- ICANN has survived a major lawsuit from VeriSign that tested ICANN's ability and right to respond to VeriSign's attempt to utilize queries to uninstantiated domains.

- ICANN has instituted the RSTEP program to examine security and stability issues associated with proposed changes to registry operations. This program was developed in direct response to the issues in the VeriSign lawsuit, part of which focused on ICANN's previous difficulties in responding to proposed changes from registries. This program uses a paid set of external consultants, operates under a tight, well-defined timeframe, and delivers carefully researched and well-written reports. Many of the RSTEP consultants are also SSAC members.

- ICANN has strengthened its internal staff with a specific role called out in the

IANA contract for a Chief Security Officer,[8] a Director of Security Operations,[9] and a Chief Internet Security Advisor.[10]

- ICANN has augmented its IANA and IT teams with specific DNSSEC expertise.[11]

- ICANN has improved its compliance efforts for registrars and registries and has developed business continuity programs for registrars and registries, including an aggressive enforcement of escrow requirements.

- ICANN created a President's IANA Consultative (PIC) committee a couple of years ago populated by a handful of Board members. The committee provided some advice to the IANA group and gained some insight into their issues. More recently, the Board created two Board level committees, a Risk Committee and an IANA Committee. The Risk Committee is focused on non-financial risks to the organization. (Financial risks are under the purview of the Audit Committee.) The IANA Committee is similar to the PIC Committee but with increased visibility to the rest of the Board.

- ICANN held a Security, Stability and Resiliency (SSR) symposium in February 2009, bringing together experts from many quarters. This provides a fresh look at what security, stability and resiliency issues are, and appears to be part of the internal initiative headed by Greg Rattray to forge a posture for ICANN and develop an agenda of specific activities.

---

[8]See section C.2.6 in http://www.icann.org/general/iana-contract-14aug06.pdf
Director of Security -- The Contractor shall designate a Director of Security who shall be responsible for ensuring technical and physical security measures, such as personnel access controls. The name of the
Director of Security shall be provided to the Government prior to contract award. The Contracting Officer's Technical Representative (COTR) shall also be notified and consulted in advance when there are personnel changes in this position.

[9]See http://www.icann.org/en/general/staff.html . Geoff Bickers - Director of Security Operations. Geoff joined ICANN in October 2008 as Director of Security Operations where he is responsible for IT security, as well as personnel and physical security matters.

[10] Ibid. Greg Rattray - Chief Internet Security Advisor. Greg joined ICANN in July 2008 as Chief Internet Security Advisor where he provides expertise on security matters both external and internal while managing the Security group.

[11]Ibid. Richard Lamb - DNSSEC Program Manager. Rick started performing IANA functions in 2007 after escaping from Washington DC where he was Director Global IT Policy at the US Department of State. While there he spent much of his time working to ensure policymakers and other stakeholders understood the technology and philosophy behind the Internet and other information technologies. Joe Abley has also joined the team and is in charge of DNSSEC Operations. His name is not yet posted on the personnel list.

- In the recent Mexico City ICANN meeting, ALAC turned much of its attention to security, forming one its five working groups to attend to DNSSEC,[12] and it held a separate session on "Registries, Registrars and the Abuse of Domains."[13]

---

[12]http://www.atlarge.icann.org/summit/wg/security-en.htm
[13]http://mex.icann.org/node/2736

Appendix 2: List of SSAC Reports, Advisories and Comments

Categorization of SSAC Reports, Advisories and Comments

Report #	Year	Type	Topic
40	2009	Report	Registration
38	2009	Report	Registration
37	2009	Report	IDN
36	2009	Comment	ICANN Plan
35	2008	Report	DNSSEC
34	2008	Comment	ICANN Plan
33	2008	Report	Whois
32	2008	Advisory	Redirection
31	2008	Comment	ICANN Plan
30	2008	Report	DNSSEC
29	2008	Comment	DNSSEC
28	2008	Advisory	Registration
27	2008	Comment	Whois
26	2008	Advisory	Registration
25	2008	Report	Fast Flux
24	2008	Report	Registration
23	2007	Report	Whois
22	2007	Advisory	Registration
21	2007	Report	IPv6
20	2007	Comment	IDN
19	2007	Comment	Root Glue
18	2007	Report	Root IPv6
17	2007	Report	Root IPv6
16	2007	Report	Root IPv6
15	2006	Report	Redirection
14	2006	Report	Whois
13	2006	Comment	Redirection
12	2006	Comment	IPv6
11	2006	Report	Registration
10	2006	Report	Registration
9	2006	Report	Alternative Roots
8	2006	Report	DDoS Attacks
7	2005	Report	Registration
6	2004	Report	Redirection
5	2003	Report	DNS Servers
4	2002	Report	Address Verification
3	2002	Report	Whois
2	2002	Report	General
1	2001	Report	General

Tabulation by Topic:

Count of Topic	Type			
Topic	Advisory	Comment	Report	Grand Total
Address Verification			1	1
Alternative Roots			1	1
DDoS Attacks			1	1
DNS Servers			1	1
DNSSEC		1	2	3
Fast Flux			1	1
General			2	2
ICANN Plan		3		3
IDN		1	1	2
IPv6		1	1	2
Redirection	1	1	2	4
Registration	3		6	9
Root Glue		1		1
Root IPv6			3	3
Whois		1	4	5
Grand Total	4	9	25	38

Appendix 3: SSAC Charter[14]

The Committee on Security and Stability will advise the ICANN community and Board on matters relating to the security and integrity of the Internet's naming and address allocation systems. Reporting directly to the Board, the Committee is chartered is to undertake the following tasks:

- To 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. The committee will focus on the operational considerations of critical naming infrastructure.

- To communicate on security matters with the Internet technical community and the operators and managers of critical DNS infrastructure services, to include the root name server operator community, the top-level domain registries and registrars, the operators of the reverse delegation trees such as in-addr.arpa and ip6.arpa, and others as events and developments dictate. The Committee will gather and articulate requirements to offer to those engaged in technical revision of the protocols related to DNS and address allocation and those engaged in operations planning.

- To engage in ongoing threat assessment and risk analysis of the Internet naming and address allocation services to assess where the principal threats to stability and security lie, and to advise the ICANN community accordingly. The Committee will recommend any necessary audit activity to assess the current status of DNS and address allocation security in relation to identified risks and threats.

- To communicate with those who have direct responsibility for Internet naming and address allocation security matters (IETF, RSSAC, RIRs, name registries, etc.), to ensure that its advice on security risks, issues, and priorities is properly synchronized with existing standardization, deployment, operational, activities and inform the ICANN community and Board on their progress, as appropriate.

- To report periodically to the Board on its activities.

- To make policy recommendations to the ICANN community and Board.

---

[14]*Bylaws For Internet Corporation For Assigned Names And Numbers*. 29 May 2008. Article XI, section 2.1 <http://www.icann.org/en/general/bylaws.htm#XI>

Appendix 4: Summary of Recommendations

The following list summarizes the recommendations made in the SSAC review of SSAC:

S 1: ICANN should see sufficient value in SSAC's independent technical fact checking.

S 2: The SSAC charter should be reconsidered as part of the regular review process.

S 3: The first item in the current charter regarding "developing a security framework..." should be removed.

S 4: SSAC has not required formal confidentiality statements to date, but has expected members to handle confidential material appropriately. Whether to require formal confidentiality agreements is worth further discussion.

S 5: Because the security professionals on SSAC know how to deal with privileged information, there is no reason that SSAC should not undertake private studies and reports.

S 6: The parts of ICANN's responsibility for security and stability, including IANA functions and internal operations, not limited by contract or employment policy should be within SSAC's review.

S 7: SSAC should avoid operational response and concentrate on systemic issues.

S 8: SSAC members should serve three-year terms, renewable by recommendation of the chair.

S 9: A membership committee should review individual contributions regarding renewal of terms.

S 10: The formality of quorum, voting, Robert's Rules, recusal, dissent, and approval are unnecessary because SSAC is not representational.

S 11: SSAC should (continue to) choose what studies to pursue.

S 12: SSAC should improve the way it informs the ICANN community of its work.

S 13: SSAC should consider which reports to ask ICANN to translate into other languages.

S 14: SSAC should consider (staffing) a continuing process of feedback from the ICANN community on its work.

S 15: ICANN should fund travel and lodging to increase SSAC members' participation at ICANN meetings.

S 16: We see no reason to either require or prohibit the same person from serving in both Chair and Liaison roles.

S 17: SSAC should conduct a dedicated meeting annually.

S 18: SSAC should prepare annual plans including projects, priorities, and resources required.

S 19: SSAC should submit a budget request to ICANN based on the annual plan.

S 20: ICANN's regional liaisons should provide periodic briefings to SSAC members.

S 21: SSAC's web site requires constant maintenance.

S 22: SSAC should consider maintaining public comments on its documents.

S 23: Executive Committee minutes should be made available to SSAC members.

S 24: ICANN should provide the reasonable resources justified in the budget SSAC prepares.

Appendix 5: Recommendations from External Review

The following list of recommendations from the external review[15] is annotated with SSAC's response and the related recommendation from our own review.

R 1: ICANN maintain an advisory body comprised of outside experts on the security and stability of the Internet's unique identifier systems.

agree S 1

R 2: SSAC maintain its fundamental identity as an Advisory Board chartered by and reporting to the Board of Directors.

agree S 1

R 3: As SSAC and RSSAC are designed for different purposes, we do not recommend the combination of these bodies.

agree

R 4: SSAC members should not be required to sign confidentiality or duty of loyalty agreements with ICANN.

agree S 4

R 5: The SSAC Charter should be amended to exclude dealings with confidential or proprietary information absent specific guidance from the Board.

disagree S 5 – Because SSAC is composed of security professionals who often deal with private information, this would unnecessarily hamper analysis by denying useful information.

R 6: The SSAC Charter be amended to exclude involvement with or review of internal ICANN operations except as specifically directed by the Board.

disagree S 6 & S 7 – 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.

---

[15] Review of the ICANN Security and Stability Advisory Committee, Final Report, 15 May 2009, JAS Communications, Inc.

SSAC Review of SSAC

R 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).

disagree – 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.

R 8: SSAC Charter be amended to add a requirement that the SSAC Chair and the SSAC Board Liaison are not the same individual.

disagree S 16

R 9: ICANN reimburse travel expenses for the SSAC Chair to ICANN meetings when appropriate.

agree but getting more SSAC members to ICANN meetings would help S 16

R 10: ICANN Board study the issue of paying a stipend or honorarium to SSAC Leadership and members.

agree

R 11: The SSAC charter be amended to specifically include nontechnical risks to security and stability as within scope.

disagree – Although non-technical risks to security and stability are considered by SSAC, its focus should remain on objective facts

R 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.

agree S 7

R 13: SSAC Leadership improve sensitivity to political and business issues by heeding the following advice (abridged).

agree – 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.

R 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.

disagree S 7 – The current charter adequately indicates that SSAC's mission is strategic rather than operational.

R 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.

disagree S 18 & S 19 – 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.

R 16: SSAC keep and publish meeting minutes on the SSAC web site in a timely fashion.

agree S 21 – With the understanding that minutes are not the same as transcripts.

R 17: SSAC should endeavor to keep their web site current to include work in progress and work planned for the future.

agree S 21

R 18: As a part of SSAC's first annual plan, SSAC revisit task area 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."

disagree S 3

R 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.

agree

R 20: SSAC membership appointments be for a term of three years, renewable by the Board at the recommendation of the SSAC Chair indefinitely.

agree S 8

R 21: Do not impose a limit on the number of terms an SSAC member may serve.

agree S 8

SSAC Review of SSAC

R 22: Stagger SSAC member terms such that roughly 1/3 of the terms are up for renewal each year.

agree

R 23: SSAC Board Liaison be permitted a maximum of three consecutive one-year terms.

disagree S 16

R 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.

disagree – 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.

R 25: SSAC implement a policy explicitly stating that the SSAC brand (written or verbal) is to be used only on approved work products.

disagree – The focus on "branding" is inconsistent with the objective fact-based approach that is SSAC's primary distinctive value.

R 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.

disagree S 10

R 27: The SSAC formally approve and release all work products pursuant to the chosen decision-making and documentation strategy.

disagree S 10

R 28: SSAC formally and visibly adopt a suitable default confidentiality policy. Other policies are used as necessary by mutual agreement.

agree

R 29: Utilize the mechanisms recommended in this review, including the annual planning process, to regularly evaluate SSAC performance against objectives and resource utilization.

disagree - evaluating performance against objectives is appropriate for employees, but not for volunteer experts often from outside the domain-name business.

R 30: SSAC publish simple conflict disclosure forms for each SSAC member on its web site. Candidate SSAC members will be required to provide a completed disclosure to the Board prior to appointment to SSAC, and shall provide an updated disclosure whenever circumstances merit.

disagree – We agree conflicts of interest should be disclosed, but prefer not to use formal, signed statements and keep these disclosures less formal.

R 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.

agree

R 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.

agree

R 33: SSAC develop and post a conflicts of interest policy based on the ICANN Board policy.

agree