Review of the

ICANN Security and Stability Advisory Committee

Prepared for the Internet Corporation for Assigned Names and Numbers

--PUBLIC DISCUSSION DRAFT #1--

16 February 2009

JAS COMMUNICATIONS LLC
INFORMATION TECHNOLOGY · RISK MANAGEMENT · GOVERNANCE

Founded in 2003, JAS Communications is a unique professional services firm delivering risk management, technology, and governance solutions to a wide range of commercial and government clients.

http://www.jascommunications.com

(*) JAS Communications LLC has previously done work for ICANN as a subcontractor to Delta Risk LLC.

Table of Contents

1 Summary

The ICANN Security and Stability Advisory Committee (SSAC) was created following the September 11 terrorist attacks as a mechanism to engage subject matter experts in the area of security. The SSAC today is an Advisory Committee to the ICANN Board of Directors providing advice and counsel on security and stability related issues.

ICANN's Bylaws describe an ongoing organizational review process as a part of its commitment to evolution and improvement. As specified in the Bylaws, the goal of the review shall be to determine:

- Whether that organization has a continuing purpose in the ICANN structure, and
- If so, whether any change in structure or operations is desirable to improve its effectiveness.

JAS Communications LLC was engaged to perform the first such review of the SSAC in November 2008. We collected qualitative and quantitative data through interviews, email communications, and an online survey instrument from just over 50 individuals and organizations in preparation for this report.

Unquestionably, SSAC has a continuing purpose in the ICANN structure. We found SSAC to be aptly filling its role as an advisory body to the ICANN Board of Directors and to the ICANN Community by providing valuable information, advice, and counsel. We found the mechanism of a Board Advisory Committee to be an appropriate model for engaging subject matter experts in the area of security and stability. While security expertise has been appropriately added on the management/staff side of ICANN, we also believe that security and stability is so core to ICANN's mission that independent sources of counsel are advisable and thoroughly appropriate. We believe that the ICANN Board and the ICANN Community will be in need of security and stability advice for the foreseeable future.

There are opportunities to improve SSAC. We identified three general areas where SSAC may be improved:

- Organizational clarity and charter
- Improving formality and transparency
- Proactively addressing conflicts of interest

We note that SSAC was created rather hastily and has evolved significantly since 2001; in the same way, ICANN has evolved significantly since 2001, including the recent additions of security-oriented management and staff. We also note that this is the first external review of SSAC. As such, we believe that the issues identified during this review are typical of "growing pains" and are relatively easily remedied now, but almost certainly will worsen if issues are allowed to fester.

Charter: Currently, SSAC's charter is overly broad and can be interpreted to include virtually any topic or activity. This is problematic and is an unnecessary source of ongoing tension. Several of our recommendations seek to clarify the charter by specifically addressing areas where there is ongoing ambiguity.

Annual Review and Planning Process: We recommend SSAC engage in an annual review and planning process together with ICANN management, staff, and the community. We believe this provides an opportunity for SSAC to coordinate with other security related activities within ICANN as well as to synchronize with the community. Additionally, the plan would improve visibility, transparency and accountability. The plan would be approved by the Board and would contain provisions to adequately resource SSAC to accomplish the tasks at hand.

Improving Internal Process: SSAC has developed a powerful and effective culture of cooperation and collegiality. We have recommended several improvements which will strengthen SSAC's internal processes without creating overbearing bureaucracy.

Conflict of Interest Practices: Outsider's perceptions of possible conflicts of interest within SSAC are problematic, but fortunately relatively easy to remedy. We recommend SSAC develop and publish a conflicts of interest policy and include discussion in every final work product about dissent or recusals during product development.

SSAC is a unique entity with a strong, positive, and productive culture. SSAC is functioning, functioning well, and filling a relevant purpose; we are confident SSAC, ICANN, and the ICANN Community will be made even stronger by acting on the recommendations put forward in this report.

1.1 Summary of Recommendations

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

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

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

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

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

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

RECOMMENDATION 7: Correct the perception of SSAC "independence" through improvements in formality, transparency, and increased Board interaction (specific recommendations in multiple locations).

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

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

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

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

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.

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

RECOMMENDATION 14: The SSAC charter be amended giving guidance to focus on issues of strategic and policy importance and to avoid tactical issues except as charged by the Board.

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.

RECOMMENDATION 16: Implementation of an annual plan will reduce the need for frequent Executive Committee and full committee meetings. We recommend reducing meeting volume to: (a) Monthly Executive Committee meetings of 60 minutes or less in preparation for (b) Quarterly full SSAC meetings of three hours or less. We recommend SSAC continue to use project-oriented SSAC subgroups.

RECOMMENDATION 17: SSAC keep and publish meeting minutes on the SSAC web site in a timely fashion.

RECOMMENDATION 18: SSAC should endeavor to keep their web site current to include work in progress and work planned for the future.

RECOMMENDATION 19: 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."

RECOMMENDATION 20: SSAC should endeavor to find the best experts globally without regard for geographic proximity. SSAC membership should not be subject to artificial geographic quotas.

RECOMMENDATION 21: The SSAC Chair establish a target size of 15 for SSAC membership; the Chair is free to operate SSAC at larger or smaller sizes as he or she see fit.

RECOMMENDATION 22: SSAC membership appointments be for a term of three years, renewable by the Board at the recommendation of the SSAC Chair indefinitely.

RECOMMENDATION 23: Do not impose term limits on SSAC members.

RECOMMENDATION 24: Stagger SSAC member terms such that roughly 1/3 of the terms are up for renewal each year.

RECOMMENDATION 25: SSAC Board Liaison be permitted a maximum of three consecutive one year terms.

RECOMMENDATION 26: 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.

RECOMMENDATION 27: SSAC implement a policy explicitly stating that the SSAC brand (written or verbal) is to be used only on approved work products, and that use of the SSAC brand outside of these official products must be approved in advance by a majority vote of the SSAC.

RECOMMENDATION 28: SSAC formally and visibly adopt Roberts Rules of Order for conducting SSAC business meetings.

RECOMMENDATION 29: SSAC formally and visibly adopt Chatham House Rule as its default confidentiality policy. Other policies are used as necessary by mutual agreement.

RECOMMENDATION 30: Utilize the mechanisms recommended in this review, including the annual planning process, to regularly evaluate SSAC performance against objectives, resourcing, and efficiency metrics in the future.

RECOMMENDATION 31: 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.

RECOMMENDATION 32: 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.

RECOMMENDATION 33: 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.

RECOMMENDATION 34: SSAC develop and post a conflicts of interest policy based on the ICANN Board policy.

2 Background

The Internet Corporation for Assigned Names and Numbers (ICANN) was formed to coordinate the allocation and assignment of the core unique identifiers on the Internet (the domain names, Internet protocol addresses and autonomous system numbers and protocol port and parameter number assignments), to coordinate the operation and evolution of the domain name system, root name server system, and to coordinate policy development reasonably and appropriately related to these technical functions. To perform its mission, ICANN adheres to a number of core values to guide its decisions and actions, including the preservation and enhancement of operational stability, reliability, security and global interoperability of the Internet.

2.1 The ICANN Security Environment

In recognition of the potential for disruptions to the Internet's systems of unique identifiers—the domain name system (DNS), Internet protocol (IP) addresses and autonomous system (AS) number allocations, and protocol port and parameter number assignments—ICANN has developed a variety of structures that address aspects of security and stability. There is presently no "one stop shop" for security considerations within the ICANN organization–in contrast, there are a number of major roles played by different players. On their face, some of these organizations may have areas of overlapping mission and responsibility. While the scope of review was limited to SSAC, this brief overview is intended to help delineate between the larger security bodies encountered during the SSAC review.

2.2 SSAC

The body currently known as the Security and Stability Advisory Committee (SSAC) began as the "President's Committee on Security and Stability." Board Resolution 01.117 - passed on November 15, 2001 - instructed the ICANN President to develop a charter for and populate this new body.[1] It is important to note that this resolution was passed during a security-focused meeting in the environment immediately following the terrorist attacks of September 11.

Resolution 02.27 - passed on March 14, 2002 - approved the Charter developed by the President, noting that Dr. Stephen Crocker was appointed Chair of the new body.[2]

The May 13, 2002 meeting minutes contain the following verbiage: "To expedite the committee coming into operation, the Board directed the President to establish the committee as a President's standing committee, with the understanding that the Board was inclined later to convert the committee into an

[1] ***Third Annual Meeting of the Board***. Internet Corporation for Assigned Names and Numbers. 15 November 2001. Accessed 11 February 2009. <http://www.icann.org/en/minutes/minutes-15nov01.htm#01.117>

[2] ***Preliminary Report ICANN Meeting in Accra.*** Internet Corporation for Assigned Names and Numbers. 14 March 2002. Retrieved 09 February 2009. <http://www.icann.org/en/minutes/prelim-report-14mar02.htm#SecurityCommitteeCharter>

advisory committee under ICANN's bylaws." [3] Resolutions 02.63-65 convert the President's Committee on Security and Stability to the SSAC that exists today.

Published minutes from both of these meetings reflect neither discussion surrounding governance issues related to SSAC, nor its proper place within the ICANN structure.

Board Advisory Committees, including the SSAC, are defined in Article XI of the ICANN Bylaws.[4]

SSAC exists to advise the ICANN community and Board on matters relating to the security and integrity of the Internet's naming and address allocations. SSAC reports directly to the Board and was, at the time of its charter, tasked with six core functions.

> 1. 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.
>
> 2. 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.
>
> 3. 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.
>
> 4. 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, and coordination activities. The Committee will monitor these activities and inform the ICANN community and Board on their progress, as appropriate.

---

[3] ***Minutes Special Meeting of the Board.*** Internet Corporation for Assigned Names and Numbers. 13 May 2002. Accessed 12 February 2009. <http://www.icann.org/en/minutes/minutes-13may02.htm#02.63>

[4] ***Bylaws For Internet Corporation For Assigned Names And Numbers***. Internet Corporation for Assigned Names and Numbers. 29 May 2008. Accessed 11 February 2009. <http://www.icann.org/en/general/bylaws.htm#XI>

5. To report periodically to the Board on its activities.

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

2.3 RSTEP

The Registry Service Technical Evaluation Panel (RSTEP) was implicitly called for by a November 8, 2005 consensus policy adopted by the Board of Directors. RSTEP was implemented in August 2006 as a reaction to specific registry needs. RSTEP is invoked when a registry submits a change request to its agreement or wishes to offer new products and services as a registry or relying on its registry status. RSTEP identifies up to five examiners from a panel of 20 experts in the design, management and implementation of complex systems and standards-protocols used in the Internet infrastructure and DNS to neutrally evaluate the registry's request against the potential for security or stability impact. RSTEP ensures that the examiner offering their expert opinion has no competitive, financial or legal conflicts of interest that could undermine the objectivity of the technical security/stability evaluation.

There is some overlap between members of the RSTEP panel and SSAC membership.

2.4 IANA Director of Security

The Internet Assigned Numbers Authority (IANA) director of security role is a requirement under section C.2.6 of the ICANN/U.S. Government contract to perform the IANA function. The IANA Director of Security is responsible for ensuring technical and physical security measures, such as personnel access controls, to protect the data and functions of IANA.

At the time of this writing, this role is performed by Barbara Roseman, the general manager of IANA.

2.5 Chief Internet Security Advisor (and Staff)

In July 2008, a staff position of Chief Internet Security Advisor (CISA) was created, reporting to the Chief Operating Officer. The CISA role directs staff security efforts within ICANN, including interfacing with SSAC. Presently the CISA is resourced with a director of internal security, the ICANN Chief Technology Officer and a pending position of Global Security Liaison.[5]

At the time of this writing, this role is performed by Dr. Greg Rattray.

[5] ***ICANN Job Vacancies.*** The Internet Corporation for Assigned Names and Numbers. 10 February 2009. Accessed 13 February 2009. <http://www.icann.org/en/general/jobs.htm#gsl>

3 JAS Review Methodology

JAS Communications initially envisioned approaching this project no differently than we have approached the other "360 Degree" technology governance reviews we have performed:

- Qualitative data collection through interviews and written feedback
- Quantitative data collected through the use of several standard team performance survey instruments
- Analysis, recommendations, and documentation

JAS was engaged immediately prior to the ICANN Cairo meeting. Data collection began in Cairo and it quickly became apparent that organizational issues would dominate our study. With so much uncertainty around scope and mission, we found it difficult to apply typical group performance metrics because there was no baseline in terms of a clear charter, specific tasking, or even agreed upon strategic direction. Put another way, it is difficult to evaluate the performance of a group when it is not clear what they are supposed to be doing. It was very clear that SSAC was working diligently, but JAS was asked whether the work it was doing was the right work.

We conceded that we would be performing a largely qualitative analysis of strategic organizational issues but specifically wanted to avoid producing a report devoid of quantitative data. Working with a noted organizational behavior expert, we designed a custom survey instrument to produce quantitative data around specific recurring organizational questions unearthed during the interviews.

The primary objective of the survey was to provide a series of quantitative tests against which to verify our qualitative observations. A secondary objective was to provide a dataset against which to run regression models while testing our recommendations. Specifically, we sought to find correlations between demographic data and areas of disagreement in order to make recommendations that will have the desired results.

Phone and in-person interviews were conducted with all individuals that were interested and made themselves available. Our questions were open ended allowing participants to interpret the question in a manner that best fit their perspective and role. Follow-up questions were asked to help ensure that the discussion stayed on track and that we gathered the necessary information from each participant. Interviews shared common elements by design to enable responses to be directly compared and contrasted. With few exceptions, all interviews were conducted with at least two JAS representatives present enabling one to take the lead and the other to document and cross-check responses in real time with previous interviews (potentially leading to clarifying questions). Several interviews were recorded with advance permission.

JAS solicited feedback in person and by email to relevant ICANN structures, the SSAC, and by reaching out to more than 100 individuals that we know are directly or indirectly involved with SSAC, we were

referred to, or through research we determined would have valuable perspective. During the Cairo meeting, JAS sent two senior representatives to raise awareness of the SSAC review and actively solicit feedback; these representatives introduced themselves during the full gNSO, ALAC, and ccNSO sessions. An open invitation for feedback by email appears on the ICANN SSAC Organizational Review web page, along with our email alias.[6] Finally, the survey permitted anonymous submission of textual commentary as well as structured data; anyone wishing to remain anonymous was directed to the survey.

Solicitation of survey responses was more controlled by design. Because it was possible to complete the survey anonymously, it seemed almost an invitation for mischief. While JAS controlled the risk through the use of a CAPTCHA, marketing the survey in an uncontrolled manner (for example by posting a link on a public web page) did not seem prudent.

After completing the initial rounds of data collection and receiving more than 20 survey responses, we began to formulate and test hypothesis and recommendations. We tested proposed recommendations against our regression models as well as through multiple rounds of interviews. For this reason, we delayed interviews with senior individuals until late in the process.

Finally, we documented our findings, analysis, and recommendations and solicited early feedback on a draft from select individuals

3.1 Peer Organizations

JAS researched peer organizations with the following characteristics:

- International in scope
- Organized as a nonprofit charitable purpose origination
- Active ("working") fiduciary Board
- Volunteer Subject Matter Expert advisory bodies to that Board

Unfortunately, very few organizations exist with those characteristics, and little detailed information is available against which to benchmark. While examples of the practices of peer organizations and relevant local law appear throughout, we thought it instructive to briefly review an advisory body to the International Red Cross, an organization to which ICANN is often compared.

The International Committee of the Red Cross (ICRC)

The closest peer entity to ICANN in several ways is the International Committee of the Red Cross. With respect to advisory bodies, ICRC has an advisory body comprised of International Advisers as follows:

[6] ***Review of the Security and Stability Advisory Committee.*** Internet Corporation for Assigned Names and Numbers. 9 December 2008. Accessed 10 February 2009. <http://www.icann.org/en/reviews/ssac/>

> *The purpose of the group of International Advisers, set up by the ICRC for a four-year period to provide it with counsel and support in its activities and policy decisions, is to seek appropriate ways to enhance respect for IHL in armed conflicts, to help the ICRC better understand and deal with the political issues it encounters in carrying out its mandate and to assist it in analyzing the environment for humanitarian endeavor.*[7]

Advisors are selected and appointed by the Board for a four year term. There are currently eleven advisors in the 2008-2011 body. Since ICRC is by charter involved in places in the world where there is conflict, advisors are selected in regions where conflict is a reality; as such, the current body includes individuals from Côte d'Ivoire, Jordan, Iran, as well as experts from the UK, US, Sweden, etc.

The group "meets twice a year for confidential discussions with members of the ICRC Assembly and Directorate." [8]

Relatively infrequent high-level meetings are typical of Board advisory committees and mesh well with typical Boards which may meet less than a half-dozen times a year. Also, the fact that the meetings are confidential is illustrative, and not atypical.

ICANN, having a more active board, will require more active advisory bodies to keep-up, as exemplified by SSAC. However, the premise is the same: the advisory body serves to provide the Board high-level, strategic advice from noted outsiders to help them be better stewards of the entity.

While ICOC specifically seeks-out members in specific geographic areas, this is more a function of their requirement for expertise and contacts in specific areas then it is an attempt for balanced geographic representation. ICOC also forces turnover on a regular basis, likely to bring new contacts and political connections.

3.2 Weaknesses

The greatest area of weakness in our analysis was that respondents were concentrated to include close members of the ICANN Community, namely: SSAC members, and ICANN Board, staff, and management. Geographically, North American and European respondents far outweighed other areas of the world.

JAS made great efforts to market the study as broadly as possible including: announcements in public ICANN meetings (ALAC, gNSO, ccNSO), posting an email address on the public ICANN Organizational Review web site, emailing all relevant ICANN structures, and through networking and seeking referrals. However, this did not translate into broad participation.

---

[7] ***International Advisers of the ICRC, 2008 - 2011.*** International Committee of the Red Cross. 01 January 2008. <http://www.icrc.org/Web/Eng/siteeng0.nsf/html/international-advisers-for-icrc-180408>

[8] ibid.

We believe this is a case of a straightforward self-selection bias where the individuals with the most at stake in SSAC, namely SSAC members themselves and the ICANN corporate structure, were the most active participants in the review. While it is important to be mindful of this bias, we do not believe it is debilitating for the purposes of this study. Additionally, the most externally-focused aspect of the review, namely the quality of the work products, was not at all in debate; individuals closer to the SSAC are more relevant sources of input for the more controversial and nuanced components of the review.

Typical organizational reviews almost always start with an accessible and well-understood stakeholder community. In the case of reviewing any ICANN structure, it can be arguably stated that the stakeholder community includes every human on planet Earth; finding an accessible and representative sample of such a broad stakeholder community is a daunting challenge.

In future studies, addressing this bias will be a function of the duration and budget of the study. For example, an organizational review spanning several ICANN public meetings would facilitate broader geographic input from the ICANN community. However, it is not clear that the results would be sufficiently enhanced to warrant the additional cost.

4 Findings

4.1 Mandate and Guidance

The March 14, 2002 action by the Board of Directors set forth the six standing task areas listed previously. We found SSAC Members and the SSAC Chair to be very conscious of the SSAC charter; in fact, SSAC regularly tests its actions against the SSAC charter. However, the current guidance is sufficiently broad and ambiguous that drawing bright lines around SSAC responsibilities is challenging. We found widely varying interpretations of SSAC's mandate within the SSAC, among the ICANN board, management, staff, and in the community. Lack of clarity is exacerbated by the reality that "security and stability" can be interpreted to include virtually any topic or activity. Lack of clarity around scope is an ongoing source of confusion and, unfortunately, in some cases a source of tension.

The SSAC is almost exclusively self-directed. Very little guidance or strategic direction is provided to SSAC from the ICANN board, staff, or policy structures. However, during our review, on February 3, 2009, the Board of Directors formally passed a resolution tasking both the SSAC and the RSSAC to complete an "overall root zone stability study" to begin immediately and provide findings and recommendations by May 15, 2009.[9] This is a recent - and thoroughly infrequent - occurrence in the documented record.

Absent regular or formal direction by outside bodies, SSAC has proactively sought-out, researched, and reported on relevant security and stability issues impacting areas of interest to ICANN. Additionally, SSAC is responsive to current events and other external stimulus when setting its agenda. Data collected by the reviewers clearly indicates that even without clear direction from the board, SSAC is active and their work is seen both internally and externally as relevant. In fact, particularly since the addition of Mr. Piscitello, the SSAC brand has become highly correlated with relevant, timely, and high quality technical reports.

We will quickly present the six task areas identified in the current SSAC charter and summarize SSAC's activities in each area; detailed discussion of SSACs activities appears in subsequent sections.

> *Task Area 1: 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.*

A "security framework" document or similar work product as described above does not appear to exist. However, SSAC appears to have created the basis of such a framework in conjunction with research into

[9] ***Preliminary Report Resolutions of Special Board Meeting.*** Internet Corporation for Assigned Names and Numbers. 10 February 2009. Accessed 11 February 2009. <http://www.icann.org/en/minutes/prelim-report-03feb09.htm>

the VeriSign "Site Finder" issue.[10] This document identifies a five-prong approach to evaluating Site Finder, but which could also apply to other potential security and stability issues addressed by SSAC.

The instruction for SSAC to "focus on operational considerations of critical naming infrastructure" is ambiguous. SSAC has typically focused more on items of larger, strategic importance rather than issues with strictly operational implications. SSAC has made repeated attempts to become involved with internal ICANN operations, however, these efforts have not lead to any significant engagement.

> *Task Area 2: 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.*

The majority of SSAC's work falls into this task area. SSAC has been highly effective communicating with the Internet technical community and operators regarding security matters. SSAC has become a respected brand in the Internet security and technical community.

> *Task Area 3: 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.*

The SSAC has certainly been proactive in their research and publications surrounding technical security issues, and we are aware of situations where SSAC has recommended audits, particularly of internal ICANN operations. However, the performance of an ongoing "risk analysis" was identified as a weakness by several members of the community, including ICANN Board members. In general, there was a feeling that SSAC produces reports that are too focused on specific technological countermeasures and miss the larger risk management issues most relevant to policy makers.

SSAC collaborated with the gNSO over 2008 to research and produce a report on Fast Flux hosting.[11]

---

[10] ***Message from Security and Stability Advisory Committee to ICANN Board.*** Internet Corporation for Assigned Names and Numbers, Security and Stability Advisory Committee. 22 September 2003. Accessed 10 February 2009. <http://www.icann.org/correspondence/secsac-to-board-22sep03.htm>

[11] ***SAC 025 SSAC Advisory on Fast Flux Hosting and DNS***. Internet Corporation for Assigned Names and Numbers, Security and Stability Advisory Committee. 28 January 2008. Accessed 13 February 2009. <http://www.icann.org/committees/security/sac025.pdf>

Task Area 4: 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, and coordination activities. The Committee will monitor these activities and inform the ICANN community and Board on their progress, as appropriate.

SSAC is certainly in communication with individuals and entities having direct responsibility for naming and address allocation matters and members of the SSAC actively participate in the standardization, deployment, and operational communities. SSAC membership is currently (and historically) well representative of these important communities.

Task Area 5: *To report periodically to the Board on its activities.*

SSAC, through the Chair and Liaison, does report to the board on its activities, however, the reporting appears to be very informal and driven by the Chair's strong personal relationships with board members. In November 2008, the Chair and Liaison roles were for the first time divided between two individuals; this has resulted in a reported increase in the level of communication formality between SSAC and the Board.

Task Area 6: To make policy recommendations to the ICANN community and Board.

SSAC does make policy recommendations on occasion; however, the consistency and effectiveness of SSAC's formal communication with the Board is in doubt. A member of the Board commented that security is a "blind spot" for them, having less to do with the quality of SSAC advice and more to do with bridging the communications gap. This Director further commented that the lack of an "active response" to SSAC advice - from the Board and the management - makes it difficult to understand the extent to which SSAC advice and counsel is being effectively consumed.

Again, it is clear that the most effective communication mechanism between the SSAC and the board is the Chair's strong personal relationships.

4.2 Indemnification

ARTICLE XIV of the ICANN Bylaws indemnifies SSAC members when acting within the scope of his or her responsibility to the maximum extent permitted by California Nonprofit Public Benefit Corporation Law.[12] While not a universal practice, this is encouraged.

[12] ***Bylaws For Internet Corporation For Assigned Names And Numbers.*** Internet Corporation for Assigned Names and Numbers. 29 May 2008. Accessed 12 February 2009. <http://www.icann.org/en/general/bylaws.htm#XIV>

4.3 Internal SSAC Organization, Population, and Processes

SSAC is composed of a volunteer Chair, vice-chair, and members; SSAC is assisted by two paid staff members: an Executive Director and a Fellow/Senior Security Technologist. All are recognized experts in the domain name, addressing, and/or security areas.

SSAC, like the other ICANN advisory and policy bodies, provides a non-voting liaison to the ICANN board pursuant to Article VI Section 9 of the ICANN Bylaws.[13] The liaison attends board meetings, participates fully in board deliberations, and is bound by the same confidentiality and fiduciary responsibilities as voting board members. The liaison is appointed annually by the SSAC and may but need not be the SSAC Chair, and may not be one of the paid ICANN staff members.

Presently, the Chair is Dr. Stephen Crocker and the vice-chair is Mr. Ray Plzak. Mr. James Galvin, an ICANN staff member, provides support to the committee as the Executive Director. Dr. Crocker was appointed Chair by the ICANN President subsequent to the November 15, 2001 board resolution which directed the creation of the SSAC and has served faithfully ever since.[14]

There are no formal elections or term limits for SSAC leadership positions. Dr. Crocker has held both the position of SSAC Chair and the Board Liaison role since the inception of SSAC until his appointment as a full Board member in November, 2008.[15] Simultaneously, Mr. Ram Mohan was appointed to the SSAC Liaison role.[16]

Prior to June, 2005, SSAC had no compensated personnel resources. On 2 June 2005, ICANN announced the appointment of its first SSAC Fellow: Mr. Dave Piscitello. At the time the position was created, it was intended that the position would be filled by a senior, highly capable person for a term of one year.[17] Mr. Piscitello's success in this role has lead SSAC to drop the one year rotation requirement as well as the term "fellow." Currently, Mr. Piscitello is on the ICANN staff with the title "Senior Security Technologist" and formally reports to Denise Michel. There is discussion about adjusting Mr. Piscitello's appointment.

---

[13] ***Bylaws For Internet Corporation For Assigned Names And Numbers.*** Internet Corporation for Assigned Names and Numbers. 29 May 2008. Accessed 12 February 2009. <http://www.icann.org/en/general/bylaws.htm#XIV>

[14] ***Minutes Third Annual Meeting of the Board.*** Internet Corporation for Assigned Names and Numbers. 15 November 2001. Accessed 10 February 2009. <http://www.icann.org/en/minutes/minutes-15nov01.htm#01.117>

[15] http://www.icann.org/en/minutes/resolutions-07nov08.htm (Retrieved February 10, 2009)

[16] http://www.icann.org/en/minutes/secretarys-notice-05nov08.htm (Retrieved February 11, 2009)

[17] http://www.icann.org/en/announcements/announcement-02jun05.htm (Retrieved February 10, 2009)

As of February 2009, there are 31 members of the SSAC.[18] The current Chair has expressed that a range of "15-20" members seems appropriate, but no hard requirements regarding the size of the SSAC exist. The reviewers note that the SSAC membership growth has accelerated over the past 2 years.

New members may be considered at any time. Any individual may request membership by asking any current member of the committee to suggest their inclusion to the committee as a whole. Additionally, the committee may solicit membership from individuals as needed. There is no prescribed term for membership on the committee. Individual members may resign at any time for any reason. The Chair, sometimes in consultation with SSAC leadership, reviews the membership from time to time, taking into account how active the members have been. The Chair will sometimes ask a member who has not been active whether he or she wishes to continue. There is no formal member review process, no formal criteria to evaluate member performance, nor is there a formal mechanism for removal of a member.[19]

The SSAC is comprised almost entirely of well known and well respected DNS-related technologists and engineers. In general, SSAC membership is U.S. and European-centric with relatively limited membership and participation from other areas of the world. With the exception of published advisories and reports previously discussed, all SSAC-related interactions we are aware of occurred in English.

SSAC membership is managed by the SSAC Chair and all members are approved by the Board of Directors, pursuant to Article XI of the ICANN Bylaws.[20] The Chair populates the SSAC on a "best effort" basis; a formal, well-defined membership strategy or target makeup does not exist. The Chair is constantly reviewing potential candidates (proactively through recruitment when a gap exists, and reactively through inquiries). The Chair selects new member candidates and grants them "Invited Guest" status. Several weeks or months elapse with the candidate(s) essentially fully engaged as SSAC members; if the Chair feels the candidate is of value, his or her name and CV will be passed to the Board of Directors (usually in a slate of several SSAC candidates) for approval. Historically, the Board has approved such recommendations without debate.

In general we find the SSAC to be an open, informal, and collegial environment well representative of the respected, high-level individuals who make-up the committee. Members interact professionally and respectfully. Internal SSAC processes are highly academic in nature with little formal process. An SSAC

[18] ***Security and Stability Advisory Committee (SSAC).*** Internet Corporation for Assigned Names and Numbers. 01 April 2008. Accessed 10 February 2009. <http://www.icann.org/en/committees/security/>

[19] Article XI, Section 4 of the ICANN Bylaws intimates that advisory board members can somehow be removed, but there is no indication of process. The implication is that advisory board members, including SSAC members, may be removed by board resolution, probably at the recommendation of the committee chair.

[20] ***Bylaws For Internet Corporation For Assigned Names And Numbers.*** Internet Corporation for Assigned Names and Numbers. 29 May 2008. Accessed 11 February 2009. <http://www.icann.org/en/general/bylaws.htm>

member (often the Chair or the ICANN Staff resource) takes the lead on a particular work product and calls on SSAC resources as they see fit. Drafts are circulated openly within SSAC and feedback is dealt-with constructively. While the vast majority of the work is completed by a small number of contributors, it is clear that any SSAC member with particular energy or expertise on a topic is given ample opportunity to contribute.

SSAC operates in a consensus-building fashion and debilitating disagreements are rare. Formal votes are rarely, if ever used. While there are clearly thought leaders on the SSAC, all members of the committee are treated equally and are encouraged to participate.

In general, SSAC lacks formal policies and procedure not imposed by the ICANN bylaws. SSAC Leadership recognizes this is not ideal and has begun working on an internal Policies and Procedures document. JAS was provided with an early draft of said document.

Executive Coordination Meetings are attended by the Chair, Vice-Chair, Fellow/Senior Security Technologist, and Executive Director. Others may be invited and attend as needed. The meetings are scheduled weekly before the regularly scheduled committee meetings to facilitate the preparation of the agenda for the upcoming committee meeting and address general logistical topics. In general, meeting agendas are not delivered significantly in advance of meetings.

The entire SSAC has a standing weekly time slot for committee meetings, usually by teleconference supported by a Jabber chat session. If there is reason to meet, the slot will be used. Face-to-face meetings are scheduled opportunistically when other meetings/events create a convenient venue. Additionally, the committee creates workgroups to focus on specific projects.

Additionally, the SSAC also holds regular public meetings. These meetings are held in conjunction with ICANN public meetings.

The SSAC has on occasion also held special meetings on particular topics. The most visible of such meetings was held prior to the publication of SAC006, *Redirection in the COM and NET Domains*, and addressed the VeriSign "Site Finder" service. This experience is discussed in greater detail in an appendix.

4.4 SSAC Work Products

Since formation, SSAC has released 35 "reports and advisories" numbered in the SAC# series.[21] The annual breakdown of reports is as follows:

[21] ***SSAC Reports and Advisories.*** Internet Corporation for Assigned Names and Numbers, Security and Stability Advisory Committee. 11 February 2009. Accessed 10 February 2009. <http://www.icann.org/en/committees/security/ssac-documents.htm>

Year	Number of Reports/Advisories Released
2001	1
2002	3
2003	1
2004	1
2005	1
2006	8
2007	8
2008	12

Table 1

The positive impact of Mr. Piscitello's addition in 2005 is obvious; Mr. Piscitello is the primary researcher and drafter for the vast majority of SSAC work products.

Regarding the technical reports, with very few exceptions, the Community perceives SSAC's work products to be of superb technical quality and almost completely if not entirely free of technical errors. The few exceptions where an individual or entity took issue with an SSAC report appeared to be more about "packaging" and "politics" than technical accuracy.

The process for releasing a work product is not formally documented. In general, the committee collaboratively determines that a particular subject is of interest and a committee member (usually Mr. Piscitello or Dr. Crocker) take the lead on the project. Drafts are circulated among the SSAC and potentially other ICANN bodies seeking comment. Because of SSAC's visibility, a completed draft is reviewed by ICANN legal counsel for the purpose of determining potential legal ramifications of the report. Counsel and the SSAC make it very clear that this review is not designed to mandate changes, but rather as a helpful review from a liability point of view given the ever present risk of litigation and other legal repercussions. Should SSAC desire no further changes after reviewing any comments from counsel, the report is posted online. Occasionally notification of the report is formally transmitted to the board resulting in a resolution accepting the report from SSAC. However, this is not a required step nor does it occur with each report. The board does not in any way "approve" SSAC reports; they are "accepted."

Almost all of SSAC's work products are technical in nature, some containing primary research. However, SSAC does occasionally release their commentary on other matters as numbered reports as well. In 4Q2008 and 1Q2009, SSAC contributed formally to the ICANN Strategic Plan for 2009-2012. SSAC comments and cover letter were released as a work product: SAC036.[22] The SSAC formed a working

[22] ***Letter from SSAC Chair Dr. Steve Crocker to ICANN Board.*** Internet Corporation for Assigned Names and Numbers, Security and Stability Advisor Committee. 30 January 2009. Accessed 12 February 2009. <http://www.icann.org/en/committees/security/sac036a.pdf>

group to solicit, assemble, and transmit feedback from SSAC members to management. According to the cover letter in SAC036, SSAC "... believe[s] the current version of the Strategic Plan incorporates many of the changes suggested by SSAC." The cover letter closes with: "This was a productive and positive experience from our point of view, and we hope we have helped improve the Strategic Plan. We look forward to similar engagement during the reviews of the Operating Plan and the Budget."[23]

Similarly, SAC034 entitled "SSAC Comment on the FY09 Operating Plan and Budget," released June 17, 2008, represents an earlier attempt to provide input to the formal ICANN planning process.[24] With the exception of feedback reports like those listed above, SSAC reports are almost entirely technical in nature, a point that both members of the community and several members of the SSAC view as a weakness. We heard from SSAC members, ICANN Directors, and members of the community that SSAC products would be substantially improved with additional policy, economic, business, and "risk management" content. However, at present, the SSAC lacks the skill-set to provide significant commentary in these nontechnical areas.

SSAC technical products are of the most direct use to members of the community including contracted parties and other sophisticated consumers. Sophisticated consumers of SSAC products include enterprises and peer organizations in the technical and security communities. A majority of work products deal directly or indirectly with protecting registrants. In general, we found that SSAC work products were by and large more technical and less actionable than desirable for the Board of Directors or ICANN policy bodies. In most circumstances, these bodies and other interested individuals receive security-related counsel through their personal relationship with the SSAC Chair or through internally available expertise.

4.5 SSAC "Independence" and "Externality"

There is a lack of clarity around how closely SSAC is aligned with ICANN - particularly ICANN management and staff. We found the issue of SSAC's perceived and actual connection ICANN to be a complex, nuanced, and energetic topic. The scenario today is strongly bifurcated: some view SSAC as being a largely independent and autonomous entity speaking only for SSAC, while others view SSAC purely as an internal ICANN structure which represents ICANN on security matters. The varying opinions and observations on this particular topic are widespread: we see differing opinions among SSAC members, ICANN Directors, ICANN Staff, and community members.

One group of opinions holds that SSAC independence (both perceived and actual) as an important source of value. This line of thinking believes that SSAC's independent and external nature allows it to

[23] ibid.

[24] ***SSAC Comment on the FY09 Operating Plan and Budget.*** Internet Corporation for Assigned Names and Numbers, Security and Stability Advisory Committee. 17 June 2008. Accessed 12 February 2009. <http://www.icann.org/en/committees/security/sac034.pdf>

provide advice and counsel without regard for political pressures. Additionally, there is a strong belief that the high-quality individuals desired for SSAC Membership would not be available if SSAC were too closely tied to ICANN and thereby encumbered by ICANN politics.

On the other hand, others view independence as evidence that SSAC is not well integrated into the ICANN structure and in general is "operating on an island." Because SSAC has a public face, there is a feeling that SSAC public communications should be coordinated and generally in-synch with other ICANN messaging. Members of ICANN management and staff shared a concern that SSAC occasionally makes their job more difficult by operating in the public eye somewhat autonomously and unpredictably.

It is critical to note that there are two facets to this discussion: perception and reality. In general, we found tremendous variance in both.

Perhaps the best way to illustrate the confusion around SSAC "externality" and "independence" is a recent example. In November, 2008, the NTIA posted a NOI regarding DNSSEC implementation at the root. For approximately 24 hours on November 20, there was a vigorous debate on the SSAC mailing list discussing the appropriateness of SSAC responding to the NTIA NOI. The arguments can be generally summarized as follows:

- "Anything we can do to help get the root signed is time well spent."
- "I'm confused. Isn't [SSAC] part of ICANN? Wouldn't it be odd for parts of ICANN to be commenting since we're obviously an involved party?"
- "...ICANN is a multi-stakeholder, bottom up process and [each] component of ICANN speaks for itself."
- "...if SSAC members have responses to the NOI regarding technical issues, it would have a stronger impact submitted as perspectives from your organizations, not as a group statement from something that's considered a part of the ICANN structure."
- "...I further believe that it would be inappropriate for SSAC to respond, as an ICANN committee, to the NOI. ICANN has already submitted a proposal that is a focus of the NOI and SSAC's responding would have the effect of ICANN responding to its own proposal."

In the end, the SSAC elected not to respond to the NOI. There was no vote or other formal undertaking on the topic, so we are left to believe this decision was driven by the Chair after reviewing the discussion.

4.6 Confidentiality and Conflicts of Interest

SSAC members know and trust each other as a result of long relationships predating SSAC, resulting in a collegial and trusting environment. In such an environment of trust, formal recognition of confidentiality and conflicts of interest is not viewed as necessary.

There is no documented confidentiality policy for SSAC members, however, there is universal agreement among SSAC members that internal SSAC communications and deliberations are to be kept confidential. However, there is no formal written notice or documentation of this policy nor are there any agreements to this effect.

An unreleased internal draft SSAC policies and procedures document provided to JAS contains the following language regarding perceived and actual conflicts of interest:

> *The committee does not ordinarily concern itself with conflicts of interest. All members are always permitted to participate in all activities. However, the committee may elect to state potential conflicts of interest as an integral part of any publication if it deems this to enhance the final result. An individual may elect not to participate in any activity of the committee at his or her own discretion.*

We observe that this is an accurate characterization of SSAC's current views on perceived or actual conflicts of interest; in practice, we find little to no formal attention to the issue. There are no formal conflict disclosure processes[25] or requirements that participants recuse themselves under certain circumstances. Committee members all know each other, who they work for, and automatically process any potential conflicts without fanfare or formality. Communications between committee members occasionally contain casual verbiage reminding folks of potential conflicts. The highly academic and technical nature of the committee combined with the notable reputations of the members and preexisting trust relationships leads to an implicit stance that overt recognition of conflicts is superfluous.

4.7 Representation and Use of the SSAC Brand

We find that the SSAC brand is a respected brand in the broader community and is highly tied to ICANN. While official work products (numbered reports) are branded SSAC, the SSAC brand also appears in other places including letters and public presentations. Not all public uses of the SSAC brand in

[25] Previously, there was a confidentiality and conflict of interest policy posted on the SSAC web site; see: ***Statement Concerning Conflicts of Interest Within the Security and Stability Advisory Committee.*** Internet Corporation for Assigned Names and Numbers, Security and Stability Advisory Committee. 2 October 2003. Accessed 13 February 2009. <http://web.archive.org/web/20040408210136/ssac.icann.org/conflict-of-interest.htm> Note that this material was no longer available from the ICANN web site. At the time of this report, no such policy was posted to the SSAC site.

presentations appear on the official "SSAC Presentations" site as the most recent presentation is dated November 2, 2007.[26] Similarly, the SSAC "projects" document appears dated.[27]

There is no formal mechanism for determining who can "speak for" SSAC, and what commentary is representative of SSAC membership. The issue of SSAC representation is of particular concern in the community with respect to the Chair and the Fellow/Senior Security Technologist; there is general confusion as to whether these individuals are speaking for themselves or on behalf of SSAC. We note that these individuals are conscientious with respect to the representation issue and we also observe that personalities and history may contribute to inaccurate predispositions on both sides of this question.

Article XI, Section 1 of the ICANN Bylaws contains the verbiage "Advisory Committees shall have no legal authority to act for ICANN, but shall report their findings and recommendations to the Board."[28] JAS' review of Board resolutions finds that most - but not all - released SSAC work products have a commensurate resolution accepting the report.

4.8 Results of JAS Survey Instrument - Descriptive

JAS created a custom survey instrument designed to add quantitative data to the observations made during the interview process. We found that in general the quantitative data supported the qualitative observations. In the following tables, we present the summary findings.

Question 1: The SSAC primarily exists to service which group?

The SSAC may serve multiple groups or constituencies. Below, we have identified six groups who may receive direct services from the SSAC, in the form of advice, presentations, publications or other work products. Please rank the order of priority/importance that each of the following groups be serviced by the SSAC. The highest priority is "1"; the lowest is "6". (n=21; sorted by mode, average)

[26] ***SSAC Presentations.*** Internet Corporation for Assigned Names and Numbers, Security and Stability Advisory Committee. 07 November 2007. Accessed 10 February 2009. <http://www.icann.org/en/committees/security/ssac-presentations.htm>

[27] ***Security and Stability Advisory Committee (SSAC).*** Internet Corporation for Assigned Names and Numbers, Security and Stability Advisory Committee. 27 March 2008. Accessed 13 February 2009. <http://www.icann.org/en/committees/security/ssac-projects.htm>

[28] ***Bylaws For Internet Corporation For Assigned Names And Numbers.*** Internet Corporation for Assigned Names and Numbers. 29 May 2008. Accessed 11 February 2009. <http://www.icann.org/en/general/bylaws.htm#XI>

Current SSAC

	Min	Avg	Mode	Max	SD
ICANN Board of Directors	1	1.71	1	6	1.28
ICANN Advisory Committees and Supporting Organizations	1	2.57	2	6	1.40
ICANN Contracted Parties	2	4.00	3	6	1.35
ICANN Staff	1	3.43	4	6	1.22
Internet Business Users	1	4.43	5	6	1.18
Internet Individual Users	1	4.86	6	6	1.49

Table 2

Ideal SSAC

	Min	Avg	Mode	Max	SD	Delta
ICANN Board of Directors	1	2.14	1	6	1.64	0.43
ICANN Advisory Committees and Supporting Organizations	1	2.57	2	6	1.33	0.00
ICANN Staff	1	3.48	4	6	1.30	0.05
ICANN Contracted Parties	2	3.95	4	6	1.13	-0.05
Internet Business Users	1	4.19	5	6	1.53	-0.24
Internet Individual Users	1	4.67	6	6	1.73	-0.19

Table 3

In the Ideal SSAC table, Delta is the change in average response between the current and ideal SSAC.

Discussion

This question asks the fundamental governance question: "to which group does SSAC exist to serve?" With a mode of 1 in both current and ideal SSAC, it is clear that there is broad agreement among respondents that the SSAC primarily exists to service the Board. The priority order for current versus ideal is nearly identical which indicates that respondents generally believe the governance structures are setup correctly. In the ideal SSAC, the priority shifted away from the Board a small amount showing a desire to reduce the focus on the Board and increase the level of service to business users, individual users, and contracted parties (in that order).

It is interesting to note that in the ideal SSAC case, there were two respondents that reversed the chart in nearly identical fashion listing SSAC's primary responsibility to Internet individual users and their #6 priority as to the Board. We will discuss the topic of "who looks out for the end user" in a later discussion.

Question 2: Please evaluate the following statements about the SSAC.

In the same way as the previous question, the left column contains your responses for the Current SSAC, while the right column contains answers for an "Ideal" SSAC as you envision it. (n=22; sorted by mode, average)

This is an Agree/Disagree question with responses on a scale of 0 - 5:

0: No Opinion (removed from summary statistics)
1: Agree Strongly
2: Agree
3: Disagree
4: Disagree Strongly

Current SSAC:

	Min	Avg	Mode	Max	SD	% Agree
Reports and Advisories offer deep technical insights	0	1.545	1	3	0.72	86%
SSAC is free to proactively identify and research potential issues	1	1.591	1	3	0.78	82%
Reports and Advisories provide actionable data to Non-ICANN policy makers	0	1.773	2	4	1.20	55%
Reports and Advisories provide actionable data to ICANN policy makers	1	1.818	2	4	0.83	82%
SSAC is transparent, balanced and unbiased	0	1.955	2	4	0.93	77%
Business failure is a stability problem and therefore within SSAC's scope	0	2.136	2	4	1.22	45%
SSAC is free to exercise autonomy and independence from ICANN	1	2.318	2	4	0.82	64%
SSAC is sensitive to political and business issues	0	2.318	2	4	0.92	45%
SSAC is a strategic/policy resource	1	2.091	3	3	0.79	64%
SSAC is a tactical/operational resource	0	2.227	3	4	1.00	45%
SSAC is directed and tasked by the ICANN Board of Directors	0	2.591	3	4	1.19	27%
SSAC is directed and tasked by the ICANN Staff	0	2.864	3	4	1.01	32%
SSAC is directed and tasked by ICANN Supporting Organizations	0	2.909	3	4	0.95	23%

Table 4

Ideal SSAC:

	Min	Avg	Mode	Max	SD	% Agree	Delta
SSAC is transparent, balanced and unbiased	1	1.09	1	2	0.29	100%	-0.86
Reports and Advisories provide actionable data to ICANN policy makers	1	1.14	1	3	0.46	95%	-0.68
Reports and Advisories offer deep technical insights	1	1.23	1	2	0.42	100%	-0.32
Reports and Advisories provide actionable data to Non-ICANN policy makers	0	1.45	1	3	0.84	77%	-0.32
SSAC is free to proactively identify and research potential issues	1	1.45	1	3	0.72	86%	-0.14
SSAC is a strategic/policy resource	1	1.45	1	3	0.58	95%	-0.64
SSAC is sensitive to political and business issues	0	2.00	1	4	1.04	64%	-0.32
SSAC is a tactical/operational resource	1	2.14	1	4	1.14	64%	-0.09
SSAC is free to exercise autonomy and independence from ICANN	0	2.18	2	4	1.07	59%	-0.14
Business failure is a stability problem and therefore within SSAC's scope	0	2.41	2	4	1.07	50%	0.27
SSAC is directed and tasked by the ICANN Board of Directors	1	2.55	2	4	0.94	50%	-0.05
SSAC is directed and tasked by ICANN Supporting Organizations	0	2.41	3	4	0.94	45%	-0.50
SSAC is directed and tasked by the ICANN Staff	1	2.77	3	4	0.90	36%	-0.09

Table 5

For both charts, the outlined block of rows have mode = 1 indicating Strongly Agree was the most frequent response. Rows in blue are statistically indeterminate between Agree and Disagree; rows in black above the blue indicate Agreement, and rows below indicate Disagreement. As in the previous charts, Delta indicates the difference in average response between ideal and current incarnations of SSAC. Delta values exceeding 0.50 are highlighted in yellow indicating a meaningful discrepancy between current and ideal.

The ideal chart has two rows with mode = 1 that are also colored blue indicating statistical indetermination even though Strongly Agree was the most common answer. This indicates a strong bifurcation in the responses as the Strongly Agree responses were balanced by Disagree and Strongly Disagree responses.

Discussion

This is the most illustrative question on the instrument. It gives us both a sense of the areas where clarity is lacking, and it gives us areas where the respondents feel the current SSAC differs from a theoretically ideal SSAC.

The data confirm the high technical quality of the reports and the self-directed nature of the SSAC, but also indicate that there is clear confusion about the core SSAC mission as nearly half of the questions result in statistical indetermination between Agree and Disagree responses. We also see that improving SSAC transparency and providing actionable data to all policymakers offer the biggest opportunities for improvement.

Question 3: What are/should be the priorities of the SSAC?

Please allocate 100 points across the following categories to represent the weight with which each priority area is/should be for the SSAC. More points means that the priority is more important. Relative point allocations are important, so please distribute the points accordingly. A blank or zero priority indicates that the particular item is not/should not be a priority for the SSAC.

If "other" has any points, please describe what that priority should be in the spaces below. (n=22; sorted by mode, average)

Current SSAC:

	Min	Avg	Mode	Max	SD
Advise ICANN Board of Directors on policy matters impacting security & stability	0	13.77	10	40	10.59
Review proposed ICANN policies for security/stability impact	0	10.45	10	33	8.28
Review current ICANN policies for security/stability impact	0	9.82	10	33	8.47
Publish security advice to the Internet at large	0	8.23	5	20	6.13
Other	0	12.59	0	100	29.45
Advise ICANN Supporting Organizations on policy matters impacting security & stability	0	8.41	0	50	11.08
Be a leading forward-looking "think-tank" for security/stability issues & research	0	4.82	0	15	4.96
Respond to Internet naming/numbering disruptions	0	4.68	0	20	7.16
Review/advise industry and other non-contracted parties	0	4.64	0	20	6.15
Review/advise ICANN contracted parties	0	4.14	0	20	5.35
Develop best practices	0	3.82	0	15	4.79
Review/advise ICANN/IANA operations (including L-Root)	0	3.68	0	15	4.68
Assess business and economic risks to security & stability	0	3.32	0	20	5.19
Promote best practices	0	3.23	0	11	4.24
Review/advise ICANN internal security	0	1.91	0	10	3.10
Review/advise non-ICANN root server operators	0	1.45	0	10	2.84
Coordinate incident response activities	0	1.05	0	10	2.44

Other:
Stub: I find it very hard to assess how the current situation is
Sorry; don't really know how to rate curent priorities
Security issues that impact on fraud and trust
ran out of ideas--just wanted to add up to 100%
Technical operation of DNS in general (including root service)
publishing highly informative reports on security and stability issues.

Table 6

Ideal SSAC:

	Min	Avg	Mode	Max	SD	Delta
Advise ICANN Board of Directors on policy matters impacting security & stability	0	14.09	25	25	8.06	0.32
Advise ICANN Supporting Organizations on policy matters impacting security & stability	0	13.45	15	50	11.94	5.05
Review proposed ICANN policies for security/stability impact	5	14.14	10	50	9.50	3.68
Review current ICANN policies for security/stability impact	3	10.27	10	25	5.34	0.45
Publish security advice to the Internet at large	0	8.45	5	25	6.16	0.23
Be a leading forward-looking "think-tank" for security/stability issues & research	0	6.68	0	25	6.14	1.86
Respond to Internet naming/numbering disruptions	0	5.41	0	20	5.89	0.73
Review/advise ICANN/IANA operations (including L-Root)	0	4.45	0	15	4.98	0.77
Assess business and economic risks to security & stability	0	4.00	0	20	4.87	0.68
Other	0	3.77	0	40	9.47	-8.82
Develop best practices	0	3.73	0	15	5.22	-0.09
Review/advise ICANN contracted parties	0	3.32	0	10	3.78	-0.82
Review/advise industry and other non-contracted parties	0	2.64	0	10	3.26	-2.00
Promote best practices	0	2.36	0	20	5.02	-0.86
Review/advise non-ICANN root server operators	0	1.64	0	8	2.51	0.18
Review/advise ICANN internal security	0	1.09	0	6	2.02	-0.82
Coordinate incident response activities	0	0.50	0	6	1.41	-0.55

Other:
Security issues that impact on fraud and trust
ran out of ideas--just wanted to add up to 100%
Technical operation of DNS in general (including root service)
writing highly informative reports on security and stability issues.

Table 7

Discussion:

These data tell us that the SSAC is seen and should continue to be a policy resource for the Board. An ideal SSAC would focus even more strongly on servicing the Board and would better interface with the other Supporting Organizations. Respondents also indicated that they would like to see SSAC as a forward-looking "think tank" in addition to providing advice to industry. Lack of clarity around SSAC mission is underscored by two write-in responses in the current SSAC indicating that they were unable to evaluate SSAC's priorities.

4.9 Results of JAS Survey Instrument - Predictive

Multiple regression models demonstrated no significant statistically predictive relationships between the demographic variables and the responses. The demographic data we collected included 25 generic position descriptions (of which the respondent could choose up to five), SSAC membership, and duration of involvement in the ICANN community. Within our sample, the responses were in general widely held and not a function of demographic data.

As the Agree/Disagree data were the most insightful, we focused on regressing these data against the demographic data. Regression models including all demographic variables never exceeded an R^2 of 0.695 indicating that in general demographic data was a poor predictor of responses. This is enlightening because it indicates that opinions were in general widely held and not isolated to specific demographic groups.

Several very weak predictors did exist and are worth mentioning. Regarding the current SSAC, gNSO members perceived that SSAC counseled non-ICANN policy makers, while non-Internet industry respondents perceived SSAC provided counsel to ICANN policymakers.

Additionally, the Board sees the current SSAC as a strategic/policy resource, and in the ideal SSAC, SSAC members wish to provide counsel to ICANN policymakers.

We wish to underscore that these are statistically weak predictive relationships.

	R2 - Current SSAC	Weak Predictor (*)
Reports and Advisories offer deep technical insights	0.532	
SSAC is free to proactively identify and research potential issues	0.576	
Reports and Advisories provide actionable data to Non-ICANN policy makers	0.695	ICANN GNSO
Reports and Advisories provide actionable data to ICANN policy makers	0.677	Industry: Non-Internet (Business Role)
SSAC is transparent, balanced and unbiased	0.464	
Business failure is a stability problem and therefore within SSAC's scope	0.404	
SSAC is free to exercise autonomy and independence from ICANN	0.191	
SSAC is sensitive to political and business issues	0.642	
SSAC is a strategic/policy resource	0.689	ICANN Board of Directors
SSAC is a tactical/operational resource	0.453	
SSAC is directed and tasked by the ICANN Board of Directors	0.352	
SSAC is directed and tasked by the ICANN Staff	0.433	
SSAC is directed and tasked by ICANN Supporting Organizations	0.454	

	R2 - Ideal SSAC	Weak Predictor (*)
Reports and Advisories offer deep technical insights	0.448	
SSAC is free to proactively identify and research potential issues	0.578	
Reports and Advisories provide actionable data to Non-ICANN policy makers	0.417	
Reports and Advisories provide actionable data to ICANN policy makers	0.624	ICANN SSAC
SSAC is transparent, balanced and unbiased	0.613	
Business failure is a stability problem and therefore within SSAC's scope	0.676	
SSAC is free to exercise autonomy and independence from ICANN	0.357	
SSAC is sensitive to political and business issues	0.547	
SSAC is a strategic/policy resource	0.613	
SSAC is a tactical/operational resource	0.533	
SSAC is directed and tasked by the ICANN Board of Directors	0.582	
SSAC is directed and tasked by the ICANN Staff	0.433	
SSAC is directed and tasked by ICANN Supporting Organizations	0.648	

(*) 95% Confidence Interval does not span zero

Table 8

4.10 SSAC Effectiveness Case Study

At no time has SSAC been more visible than in September and October of 2003 during the VeriSign "Site Finder" discussions. JAS reviewed SSAC's significant involvement in this incident because it was a case study of SSAC in the limelight highlighting SSAC's public role, the ICANN board's interaction with SSAC, and their consumption of SSAC's expert security and stability advice. It was also an example of a somewhat autonomous SSAC, driven by a strong Chair, taking a leadership role in a very public forum. Finally, the numerous written communications which occurred during the period also gave insight into the working relationship between SSAC, ICANN management, and the ICANN board.

It is clear from this incident that SSAC provided a valuable and actionable source of information to the ICANN board and to the community. While numerous technical organizations provided input, it is clear that SSAC's status as an advisory body to ICANN was of unique value. SSAC was uniquely positioned to give ICANN the support it needed to take the actions it deemed necessary.

ICANN staff with expertise in security and stability has significantly increased since this incident. However, it is unlikely that management and staff alone could have brought to bear such a broad and deep pool of expertise on such short notice.

During our interview process, numerous individuals representing all areas of the community commented that the "Site Finder" episode was a "shining moment" for SSAC and that "SSAC worked extremely well in a crisis."

Some issues, particularly around SSAC's internal processes and population, were identified through this experience. We note that the RSTEP process essentially grew out of SSAC's involvement in the "Site Finder" episode. RSTEP was designed to address the organizational shortcomings of SSAC, namely SSAC's inability to deal with confidential and proprietary information, the presence of perceived and actual conflicts of interest, and the inability to demand time-delimited results from volunteers.

5 Analysis and Recommendations

5.1 Overview and Key Issues

In general there was very little disagreement about issues regarding SSAC. In fact, there was broad agreement throughout all stakeholder communities about the areas that are working well and the areas providing opportunity for improvement. JAS believes that the general SSAC model makes sense and is working. We believe that with relatively minor changes the SSAC can be made even better.

During our interview process and while analyzing the survey instrument, JAS Communications identified several recurring themes:

- Lack of organizational clarity and charter
- Lack of formality leading to concerns about transparency
- Perceived and actual conflicts of interest

The review team believes that by addressing issues in each of these three areas SSAC can be substantially improved.

5.2 Organizational Clarity and Charter

Lack of organizational clarity regarding security roles and responsibilities within the ICANN structures is the root cause of several second-order problems. SSAC's position as an Advisory Committee to the Board of Directors in and of itself creates confusion due to lack of clarity regarding their relationship with management, staff, and other elements of the ICANN ecosystem.

The SSAC appears to have been developed with some haste in the aftermath of the terrorist attacks of September 11; the fact that it was initially created as a President's Committee - "to expedite the committee coming into operation" - and converted less than six months later to a Board Advisory Committee is insightful.[29] The minutes do not reflect discussion surrounding the governance aspects of this advisory committee and how it should fit within the ICANN structure. Additional insights into the intended organizational role of the SSAC are apparent in the February 24, 2002 letter from ICANN President Stuart Lynn; however, it is also clear from this letter that ICANN was in a state of significant change.[30]

---

[29] ***Minutes Special Meeting of the Board 13 May 2002.*** Internet Corporation for Assigned Names and Numbers. 13 May 2002. Accessed 11 February 2009. <http://www.icann.org/en/minutes/minutes-13may02.htm#02.63>

[30] ***President's Report: ICANN – The Case for Reform.*** Internet Corporation for Assigned Names and Numbers. 24 February 2002. Accessed February 11, 2009. <http://www.icann.org/en/general/lynn-reform-proposal-24feb02.htm>

We believe that given this background it is appropriate to review SSAC from the ground up.

JAS Communications' experience with volunteer nonprofit organizations consistently finds that organizations in the "start-up" phase typically start with only a Board of Directors and limited to no funds for management and staff. As such, the Directors form a highly engaged "working Board" and carry-out most of the organization's work themselves. Working committees of non-Directors typically are coordinated by and report to the Board of Directors by default.

As the organization grows, management and staff resources become available. It is then appropriate for the Board to morph into a more typical high-level body charged with hiring and overseeing management and providing high-level counsel on strategic issues. At this point, external advisory committees typically become the responsibility of Management and are no longer maintained by the Board of Directors.

Good governance practice dictates a "trust but verify" relationship between the Board and management; as such, board activities are typically focused in two areas: (1) hiring and compensating management, and (2) oversight and audit to assure that management is performing as expected.

ICANN is indeed very different today than it was when the SSAC was chartered in 2002. The SSAC was chartered at a time when ICANN staff numbered less than 30.[31] Today, ICANN staff as grown to approximately four times the 2002 levels. Additionally, ICANN has moved through significant restructuring and has had multiple changes in leadership. Beginning with the appointment of the first SSAC Fellow in 2005, ICANN has made clear efforts to develop management and staff resources to address the security aspects of ICANN's mandate.

QUESTION: Is ICANN in need of an external advisory body focusing on security and stability?

The fundamental purpose of advisory boards is to allow an entity to benefit from knowledge and expertise outside of the institution. Given the massive breadth and scope of the Internet's unique identifier systems, ICANN benefits greatly from the participation of globally recognized experts. These experts represent a number of diverse and relevant fields and are employed by a number of entities including for-profit, nonprofit, educational, and government. All of these valuable positions cannot possibly be represented within staff.

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

[31] ***Preliminary Fiscal Year 2002–2003 Budget .*** Internet Corporation for Assigned Names and Numbers. 30 March 2002. Accessed 10 February 2009. <http://www.icann.org/en/financials/preliminary-budget-30mar02.htm>

Currently, the SSAC is structured as an advisory committee to the fiduciary board. In a mature and sophisticated for-profit organization, it is rare to find an external advisory board reporting to the fiduciary board; almost all such bodies are created and maintained by management. Nonprofit organizations tend to have a higher instance of such constructs, particularly in the medical field where fiduciary boards often have advisory boards comprised of well known doctors and researchers expert in topics core to the mission of the entity. As discussed previously, the International Red Cross also has such a body.

QUESTION: Is an advisory committee to the fiduciary board the right place for SSAC?

Article I, Section 1 of the ICANN bylaws starts with the sentence: "The mission of The Internet Corporation for Assigned Names and Numbers ("ICANN") is to coordinate, at the overall level, the global Internet's systems of unique identifiers, and in particular to ensure the stable and secure operation of the Internet's unique identifier systems." Article I, Section 2 states that ICANN's first Core Value is: "Preserving and enhancing the operational stability, reliability, security, and global interoperability of the Internet."[32] This is a clear indication that security is core to the ICANN mission; in fact, it can be read that ICANN is fundamentally in the business of security and stability.

Under this premise, we believe the ICANN Board requires a source of exceptionally high quality security advice which is external to and independent of management. The Board of Directors is charged with hiring and overseeing the management, and providing counsel on high-level strategic issues. Given that security and stability of the Internet's identifiers is such a crucial part of ICANN's mission, it is reasonable and appropriate that the Board of Directors have an independent source of security counsel.

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

QUESTION: Should SSAC be combined with RSSAC to form a joint "Technical Advisory Committee?"

The Root Server System Advisory Committee (RSSAC) and SSAC have recently been tasked by the Board to perform a joint project. Noting that SSAC and RSSAC have successfully collaborated in the past, it is reasonable to consider whether the two committees should be combined.

The purpose of the SSAC is to provide the best possible advice on a specific range of topics, namely those impacting security and stability. SSAC is therefore an advisory body by definition, drawing members from a wide spectrum of institutions. This is very different from the RSSAC which is designed

[32] ***Bylaws For Internet Corporation For Assigned Names And Numbers.*** Internet Corporation for Assigned Names and Numbers. 29 May 2008. Accessed 10 February 2009. <http://www.icann.org/en/general/bylaws.htm#I>

to represent a very specific group of individuals - the root server operators. RSSAC is therefore a representative body whose function it is to consider issues impacting the institutions they represent, and to serve as a communications conduit between each other and the ICANN Board.

We therefore do not advise the combination of these entities as they are designed for different purposes.

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

SSAC has a highly visible public face and a respected public brand; these features distinguish SSAC from every Board advisory committee we could find. A body created to provide advice to a fiduciary board *and to the public* is a tricky proposition as both entities have distinct public faces. This scenario creates the very real possibility of an awkward public disagreement between the Board and one of its advisory bodies.

While not inappropriate for the unique ICANN model, JAS believes that this atypical governance feature is and will continue to be a fundamental source of tension within ICANN.

Of course, all fiduciary boards have disagreements with management from time to time, but these rarely become public for a variety of reasons including a shared duty of loyalty to the entity. Additionally, confidentiality agreements are almost always in place for fiduciary directors, management, and external advisors creating an enforcement mechanism for controlled information dissemination.

Absent confidentiality agreements and a shared duty of loyalty, a public-facing advisory body may begin to look and feel more like a "watchdog" than a trusted source of advice and counsel. The term "ICANN's Regulatory Agency" was used during our interview process. While some members of the community are enthusiastically supportive of SSAC having a certain "watchdog" capacity, the majority recognize that an open relationship between SSAC, management, and the Board is more productive.

QUESTION: How should SSAC balance providing advice to the Board, management, and to the public?

Because of the very open and debate-driven nature of ICANN, we believe SSAC - using the SSAC brand - can and should participate in public ICANN discussion. However, as an advisory body, participation using the SSAC brand must be mindful, coordinated, and balanced with a sense of loyalty to the ICANN Corporation they advise. Of course, individual SSAC members acting on their own or under the brand of their employer can and should participate in any way they see fit. The only question at hand is interaction using the SSAC brand.

QUESTION: What is SSAC's role in Internet stewardship?

A recurring theme emerged regarding SSAC's role in the stewardship of the Internet. We found a not insignificant minority of respondents, inside and outside of SSAC, that see SSAC as having a "watchdog" role (official or implied) to look-out for the "interests of the Internet" independent of other entities including the ICANN Corporation and the ICANN Community.

From a governance perspective, it is clear that the ICANN Board of Directors are the fiduciaries for the ICANN mission. The Board, and ICANN in general, has been painstakingly constructed to handle this daunting task. SSAC provides the best advice possible to the Board, and the Board has the responsibility to exercise the Duty of Care to make the best decisions they can given the information they have. SSAC has an important advisory charge but no fiduciary charge.

SSAC cannot have a "watchdog" function; this is unworkable from a governance perspective, and, more practically, would destroy the valuable source of counsel SSAC provides to the Board.

As was stated previously, individual SSAC members acting on their own or under the brand of their employer can and should participate in any way they see fit. The ICANN multi-stakeholder and conflict resolution model provides numerous mechanisms for those with concerns to be heard - from participation in the policy development process to the Ombudsman / Alternative Dispute Resolution (ADR) process.

There is no recommendation attached to this discussion; we believe it important background information for subsequent discussion. We believe recommendations made elsewhere in this study will address this particular problem.

QUESTION: Are confidentiality agreements or written pledges of loyalty appropriate for SSAC members?

It is not atypical for advisory board members to have agreements with the entity they advise including confidentiality provisions and language asserting a duty of loyalty. However, we believe that in the ICANN model, such agreements would not be of meaningful benefit and would come at a significant cost in terms of SSAC participation and public perception. As such, we do not recommend SSAC members be required to sign agreements of any kind.

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

However, because of the lack of confidentiality agreements and potentially conflicting duties of loyalty (SSAC members are often employed by entities party to agreements with ICANN), some refinement of SSAC scope is necessary.

We believe SSAC should be free to comment on publically available information and conduct primary research, however, it is not appropriate for SSAC to deal with confidential or proprietary information

absent specific guidance from the Board. Perceived and actual conflicts of interest and the lack of confidentiality agreements simply make this unworkable. JAS notes that the RSETP process was essentially invented to address this particular weakness through short-term purpose-built consulting contracts with high-level experts, many of whom are also SSAC members.

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

A certain sense of "tension" between directors (and their advisory bodies) and management is healthy and should be present when good governance practice is in place. The reviewers occasionally detected tension between management and the SSAC - most normal and healthy; much of the rest can be largely attributed to a mutual lack of mission clarity. One of the areas lacking clarity is the extent to which SSAC should be involved with internal ICANN operations.

QUESTION: What is SSAC's role with respect to internal ICANN operations?

Like any business, ICANN is in possession of confidential and proprietary data, and data protected by law. Examples include personnel records and internal business communication. Additionally, ICANN views operational elements of the various root zone management processes as sensitive and proprietary. We feel it is therefore unworkable for SSAC to become directly involved with day-to-day ICANN operations.

JAS believes that ICANN's internal operation needs to fall outside the scope of SSAC's charter. Examining internal operations would appear to be a review of the specific tactics being undertaken by management. We see review of such concerns to fall closer to the role of "audit" than "strategic analysis and recommendation." While it certainly is appropriate for SSAC to advise the Board to commission audits of ICANN operations (under Article XI, section 2(a)(3)), the Board is not obliged to act on this advice, charge SSAC with performing the recommended audits, or share the results with SSAC members.

In a mature corporate entity, operational issues are under the purview of management; the Board only becomes involved in an audit and oversight capacity. It is well within the Board's authority and duty of care to occasionally review internal operations. This seems especially appropriate for ICANN given that their unique operational role comprises such a critical component of ICANN's mission.

However, the purpose of such a review is to make the Board aware of potential issues such that they can be remediated in such a way that the corporation is not damaged; the purpose of such a review is specifically not to make the *public* aware of any issues. The purpose of the advice the Board receives from Board advisory committees is to enable the Board to make better decisions, not to affect public perception of ICANN. Additionally, it is appropriate to treat tactical operational security issues as

confidential. Thus, the lack of enforceable confidentiality agreements is a nonstarter for any such review.

While one might argue that using the "ongoing threat assessment and risk analysis" component of the SSAC charter and SSAC's duty to "advise the ICANN community" about principal threats to security and stability, putting one portion of the organization (SSAC) in a position where it directly and publically critiques the core business of the whole organization is an untenable situation which would redefine SSAC to include some kind of “watchdog” responsibility. This inappropriately overlaps with existing governance and conflict resolution mechanisms within ICANN. Ultimately, SSAC's governance role in the broader security elements of ICANN's mission is to provide strategic advice and to facilitate an adequate understanding of the security and stability subject matter so as to enable the board to make the best possible decisions.

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

That being said, we reiterate that it is completely appropriate for the Board to occasionally review operational issues; if and when the Board elects to review aspects of ICANN's internal operations, we recommend an "RSTEP-like" process where individuals are selected and contracted specifically to perform such a review and report to the Board. Like RSTEP, it is reasonable to assume that several SSAC members would be involved in this capacity. These individuals will be under a contract including confidentiality provisions sufficient to protect the corporation.[33]

It would furthermore be reasonable and appropriate for SSAC to be consulted during the crafting of such an engagement.

QUESTION: To what extent is SSAC "independent" from ICANN?

Closely related to SSAC's position within ICANN is the issue of SSAC's "independence" from ICANN. We believe that SSAC has nurtured the perception that SSAC is somewhat "outside" of ICANN for several reasons. First, as a recruiting tool; there is a belief that the type of industry experts required to make SSAC successful would be skittish of being tied too closely to ICANN. Secondly, the perception of externality permits SSAC's powerful brand to be used to comment freely (and publically) on ICANN. Unfortunately, in isolated cases, lack of clarity around the issue of independence has also resulted in suspicion and mistrust.

[33] JAS notes that an aggressive interpretation of ICANN’s Bylaws, article XI-A section 1.6 (<http://www.icann.org/en/general/bylaws.htm#XI-A>) could require a confidential report to the Board be opened for public comment by other advisory committees and supporting organizations. Addressing this concern is beyond the scope of this review.

The perception of independence is not universally shared; nowhere was this more clear than the November 2008 NTIA NOI comment period discussed previously. Qualitative data suggest that members of the SSAC view SSAC more externally than does the ICANN management, staff, and the rest of the community. Additionally, we believe that personalities and history lead to inaccurate predispositions on both sides of this question.

In reality, SSAC has historically been permitted to act autonomously, with limited transparency, little formality, and to be almost exclusively self-tasking within a broad strategic charge. Use of the SSAC brand has not been carefully controlled by the Board. As such, it is easy to understand the perception of "independence."

JAS believes that the issue of "independence" and "externality" must be immediately put to rest. As an Advisory Committee to the Board of Directors, SSAC is most certainly a body within ICANN. SSAC receives significant[34] resources from ICANN including the bulk of two FTE, meeting space, web presence, and other assistance. Pursuant to SSAC's charter, SSAC "reports directly to the Board;" as an advisory committee to the Board, it may also be directed by the Board.[35] There is no ambiguity; SSAC is certainly not "independent" or "external" to ICANN. SSAC does however have the ability to set its own agenda, function relatively autonomously, and express a full range of opinions.

The legal and organizational argument is not at all unclear; this issue must be remedied through process and cultural adjustments. We believe the perception of "independence" can be remedied by the Board taking a more active interest in SSAC's activities, and by improvements in SSAC's formality and transparency.

RECOMMENDATION 7: Correct the perception of SSAC "independence" through improvements in formality, transparency, and increased Board interaction (specific recommendations in multiple locations).

Issues of formality and transparency improvements will be discussed in a later section.

The SSAC Chair has a very influential role. The roles of SSAC Chair and Board Liaison are separate on paper - the same individual need not serve in both capacities. However, historically Dr. Crocker has held both positions for the vast majority of the existence of the SSAC. Dr. Crocker's valuable personal

[34] "Significant" is not in any way intended as a comparison to other components of the ICANN structure, but rather "significant" in that SSAC is resourced by ICANN to the extent that SSAC would not exist in its current form absent ICANN resourcing.

[35] ***Security Committee Charter.*** Internet Corporation for Assigned Names and Numbers. 14 March 2002. Accessed 11 February 2009. <http://www.icann.org/en/committees/security/charter-14mar02.htm>

relationships with Board members have, by far, been the most effective communication mechanism for Board level discussion of security matters.

Dr. Crocker's long service and unique (and historical) luminary status have been of immeasurable value to ICANN and to SSAC. However, consolidation of these roles has had the effect that many find Dr. Crocker so tightly associated with the SSAC that it is hard to distinguish the two. Furthermore, early indications are that the formality of communications between the Board and the SSAC have already begun to improve after the separation of these positions in November, 2008.

QUESTION: How should the Board increase its level of interaction and formality with SSAC?

Moving forward, we believe all Board/SSAC communications should decidedly *not* be consolidated in one individual. It is valuable that both the SSAC Chair and Board Liaison, having significant influence on the direction of SSAC, develop personal relationships with Board members and be involved in Board discussions whenever possible and appropriate. We believe these connections between the SSAC and the Board are of significant value, particularly for an issue as important and prevalent as security and stability.

We therefore recommend that the SSAC Chair be a distinct individual from the SSAC Board Liaison.

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

We believe it valuable to cultivate multiple relationships between the SSAC and the Board as we find that such informal relationships are a critical means of conveying advice and counsel - particularly about complex and nuanced security and stability topics. As a Board Observer, the SSAC Liaison is entitled to receive travel reimbursement for travel to ICANN board meetings; we recommend that ICANN also reimburse travel expenses for the SSAC Chair to ICANN meetings when appropriate. Having two interfaces to the SSAC will improve communication and coordination between the Board and the SSAC; the best way to encourage and cultivate these relationships is through face-to-face interaction.

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

ICANN has had the good fortune of having a highly engaged and available Internet luminary at the helm of the SSAC for more than seven years. Obviously this is not a sustainable model; to put it frankly, there is only one Dr. Crocker. Given the critical nature of security and stability to ICANN's mission, the Board must actively seek sources of exceptionally high quality security advice and counsel independent of management. Cultivating multiple relationships within SSAC is one such way to ensure that there is an adequate pool of such critical, high quality counselors.

Additionally, we recognize that Dr. Crocker has been exceptionally available during his years of service devoting inordinate amounts of volunteer time to ICANN. The Board must consider that future scheduling availability of volunteers with similar levels of expertise is likely to be less - possibly dramatically so. As such, the Board may want to consider a stipend or honorarium for serving as SSAC Chair, Liaison, and/or an SSAC member as a way to both encourage and reward participation.

It is extremely difficult to get consistent levels of engagement through strictly volunteer efforts. It is not atypical for outside advisors to be paid for their service, typically on a per-meeting basis. As any payment for service on an advisory board creates political and "slippery slope" issues, JAS recognizes that this is a complex issue requiring further study.

Payment for volunteer service is often less about the actual dollars and more about recognizing the economic value of the contributions; JAS has seen examples in other organizations where honorariums are donated to charity in the name of the volunteer.

The reviewers note that compensation of advisory board members is currently prohibited by Article XI Section 6 of the ICANN Bylaws.[36]

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

QUESTION: How should SSAC's charter be clarified?

Interviews and written responses illustrated clearly differing opinions concerning SSAC's strategic fit and role within the ICANN security apparatus. JAS' quantitative instrument underscored the statistical variance in perceptions of the fundamental SSAC charter; there was statistical indetermination on the following Agree/Disagree questions regarding the current incarnation of SSAC:

- "SSAC is free to exercise autonomy and independence from ICANN"
- "Business failure is a stability problem and therefore within SSAC's scope"
- "SSAC is sensitive to political and business issues"
- "SSAC is a strategic/policy resource"
- "SSAC is a tactical/operational resource"

[36] ***Bylaws For Internet Corporation For Assigned Names And Numbers.*** Internet Corporation for Assigned Names and Numbers. 29 May 2008. Accessed 7 February 2009. <http://www.icann.org/en/general/bylaws.htm#XI>

The reviewers found these results to be consistent with the areas revealed to be lacking clarity during the interview process. As the question of "independence" was previously addressed, we will take-up the remaining issues here.

QUESTION: Should non-technical (specifically business, economic, and legal) risks to security and stability be within SSAC's scope?

The reviewers note that the current SSAC charter contains no limitation to address only *technical* risks to security and stability. In fact, the current language in task area three contains the mandate: "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 specific direction to "determine where the principal threats to security and stability lie" reads much more broadly than just technical issues.

While the SSAC has historically focused on technical issues, we see no language in the current charter requiring such a limitation. We believe that SSAC's strong roots in the technical and engineering community, combined with strong technical leadership, has caused SSAC to focus almost entirely on technical issues.

Many risks to the modern Internet's naming and address allocation systems are not technical in nature. As the Internet has grown, so to have the range of vectors bad actors will leverage for nefarious purposes. Additionally, a large and rapidly growing number of ICANN contracted parties, a hypercompetitive naming market, IPv4 depletion, and growing namespace complexity all point to subtle and unforeseen nontechnical failure modes in the future. It is reasonable and appropriate that the Board have a source of expert advice on such topics.

Additionally, nontechnical points of view represented within SSAC work products may make them more palatable to a wider audience and would likely increase their direct value to the Board and to the community.

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

SSAC does not currently have the capability to address nontechnical issues; this topic will be discussed in a later section.

QUESTION: To what extent should SSAC become involved in law enforcement and national security issues?

We believe that SSAC's role is to research, understand, and report on issues impacting the security and stability of the Internet's unique identifier systems. Expanding the charter to include nontechnical risks admittedly may open a "slippery slope" where SSAC could find itself involved in issues that are

fundamentally under the purview of law enforcement, or issues which involve conflicts between state actors. These are areas presumably where neither ICANN nor SSAC wish to become involved.

We draw the distinction between strategic research and understanding of issues versus tactical response and mitigation. We recommend that SSAC focus on developing knowledge and understanding of risks, sharing knowledge, and making recommendations; we recommend SSAC specifically avoid tactical involvement in response or mitigation activities.

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.

QUESTION: What is the right level of SSAC sensitivity to political and business issues?

It is necessary for groups with security and stability responsibilities to ask hard and unpleasant questions. Considerations around security and stability are often at odds with business, economic, and policy agendas. This reality is not unique to ICANN.

With few exceptions, we believe that in general SSAC has been sensitive to business and political issues. We believe recommendations found elsewhere in this paper will help remedy any perception of insensitivity, specifically:

- A closer relationship with the Board and Management
- Improved clarity in the SSAC charter
- More formal internal processes and transparency
- A board-approved annual plan available to the public
- Increased visibility into resource utilization and accountability for resource consumption

Additional recommendations take the form of advice to future SSAC leadership.

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 conduct itself with the highest level of professionalism and integrity.**

There is some disagreement concerning where SSAC's activities should lie on a continuum ranging from tactical/operational concerns to strategic/policy issues. First, we must derive a working distinction between strategic and operational:

Strategic	Tactical
Project timeline measured in years	Project timeline measured in days and weeks
An exercise in resource allocation	An exercise in planning and logistics
Leadership	Management

Table 9

We observe that, with a few notable exceptions, the vast majority of SSAC's work has been on items of strategic and policy importance.

A properly functioning Board of Directors spends the vast majority of its effort considering strategic issues. As an advisory body to the Board, it is appropriate for SSAC to also focus on strategic issues in order to best provide relevant strategic advice to the Board. Additionally, volunteer advisory boards are typically unequipped to address tactical operational issues, and we find SSAC to be no exception.

In its public-facing capacity, we believe it is also appropriate for SSAC to remain focused on strategic issues as tactical and operational issues are the appropriate purview for ICANN management and staff. As discussed previously, we believe it unworkable for the SSAC to become involved in ICANN internal operational issues. We believe that these clarifications together with the volunteer nature of SSAC make it effectively unworkable for SSAC to become involved in tactical and operational issues.

RECOMMENDATION 14: The SSAC charter be amended giving guidance to focus on issues of strategic and policy importance and to avoid tactical issues except as charged by the Board.

By far, the most effective communication mechanism between SSAC and the current Board are the personal relationships and effective communication style of Dr. Crocker. We believe a focus on strategic issues, coverage of both technical and nontechnical risks, and increased SSAC attention on creating products accessible to policy makers will help increase the level of board engagement.

QUESTION: How would the creation of a board level risk committee (as recommended by the board review team) affect SSAC?

The ongoing ICANN Board of Directors review has recommended the creation of a board risk committee; this is a popular and appropriate governance mechanism which is seeing increased popularity in both nonprofit and for profit institutions. The purpose of a board-level risk committee is to enable systemic management of enterprise-wide risks facing the organization. Note that a board risk committee, like other board committees, would be comprised entirely of ICANN directors, distinguishing it from an advisory committee like SSAC.

JAS supports the creation of a board risk committee and sees SSAC as a valuable source of counsel for this new committee. We believe that a small committee comprised of interested Directors will help remedy the security "blind spot" communicated to us by a Director. The Board reviewers say the following regarding the risk committee:

> *We support the creation of a risk committee if scope is carefully defined in terms of keeping an eye on the major risks facing ICANN. These would include major political risks, technical risks, business risks, key relationships risks and the like. It would also include oversight of the processes adopted by management for dealing with operational risk, health and safety, and environmental risk etc. Less than half of the board as well as the management believe that the board 'has adequate focus on the major risks facing ICANN'*[37]

We believe that such a board committee would be ideally positioned to receive and act on SSAC advice. Further discussion and recommendations regarding the Board of Directors is out of scope for this report.

5.3 Formality and Transparency

Historically, the SSAC has been permitted to act autonomously and to be almost entirely self-tasking. While not burdening SSAC with a substantial increase in administrative requirements, we believe that SSAC, ICANN, and the community would benefit from an increased level of formality, planning, and processes. We observe that some individuals - inside and outside of SSAC - perceive the lack of formal processes and the reliance on the judgment and discretion of the Chair as a lack of transparency.

QUESTION: What is the right level of formality and planning for SSAC?

[37] ***Independent Review of the Board of ICANN Main Report.*** Boston Consulting Group. 02 November 2008. Accessed 12 February 2009. <http://www.icann.org/en/reviews/board/report-02nov08-en.pdf>

As a part of the "ongoing risk assessment" mandated in the SSAC Charter, SSAC must be free to determine what topics require attention and to allocate resources appropriately. A significant part of SSAC's value is its ability to proactively identify and research potential risks. As such, "over planning" of SSAC would hamstring its efforts and limit its value.

At the same time, a level of planning greater than what exists today is appropriate and would greatly improve coordination, resource allocation, and accountability. Additionally, numerous individuals stated a desire to see SSAC execute against a published plan.

We are sensitive to avoiding formality and process for the sake of formality and process; there are three primary justifications for an increased level of SSAC formality:

- A significant number of individuals outside of SSAC and some on SSAC perceive the lack of formality and lack of process as an uncomfortable lack of transparency. This perceived lack of transparency is at times debilitating and is damaging SSAC.
- A degree of formality and process is required to make SSAC sustainable. Currently, nearly all vital institutional knowledge rests without documentation in the minds of a very few individuals.
- Formality and process are invaluable if SSAC were to find itself in trouble. Lack of formality and process may make SSAC's actions seem arbitrary. The reviewers note that during the VeriSign SiteFinder litigation SSAC process was a subject of discussion. We also note that the ICANN Bylaws indemnify SSAC members; however, individuals must be "acting within the scope of his or her responsibility" in order to be protected.[38] Currently, determining and documenting an SSAC member's scope of responsibility and whether they are acting within it would be challenging.

We therefore recommend that SSAC commence an annual planning and reporting process. The annual plan would set forth its high-level research and publication agenda for the year, membership strategy, and resource requirements. This process, completed in conjunction with the ICANN Board and staff, will significantly improve coordination and reduce the risk of overlapping and duplication of efforts. Additionally, a planning process would allow SSAC to survey other industry efforts and take related and relevant activities into account. Several individuals interviewed by JAS noted that SSAC and ICANN would benefit from better coordination with industry activities outside of SSAC.

The annual plan will also include resource requests including telecommunications resources, meeting space, a budget for externally commissioned research and support, and other resources SSAC requires to operate. Formal accounting for SSAC's resource utilization will dramatically improve the ability for the Board to effectively manage the SSAC, and for the public to feel at ease with SSAC's activities. We believe that this approach has the opportunity to resource SSAC to a higher level than it is currently

[38] ***Bylaws For Internet Corporation For Assigned Names And Numbers.*** Internet Corporation for Assigned Names and Numbers. 29 May 2008. Accessed 10 February 2009. < http://www.icann.org/en/general/bylaws.htm#XIV>

while adding important coordination and accountability mechanisms. We also believe this process will have the effect of making SSAC service even more attractive to valuable members of the community given the ability to participate in primary research and potentially become a vector to publish academic papers and even work on a PhD thesis.

The annual plan will also include a strategy for addressing SSAC membership over the year. A planned approach to SSAC membership will make the membership process more transparent (a recurring concern) and will allow membership strategy to take into account the research agenda. For example, a year with several projects on the research agenda with economic facets may result in recruiting an Economist (or an interested economics graduate student) to serve on the SSAC as a member or guest.

Typical of the ICANN consultation model, development of the annual plan would contain a public comment period. We believe the public comment period both valuable and appropriate given SSAC's dual mandate to provide advice to the Board and the public. Finally, the annual plan would be formally presented to the Board for approval thus granting SSAC a clear annual mandate and authorizing the use of resources.

In conjunction with the annual planning process, the SSAC shall also report on the activities of the previous year. This closed-loop approach to planning and review dramatically improves accountability, transparency, and elevates the level of synchronization between SSAC, the ICANN Board, and ICANN staff. We believe this critically important given ICANN's development of an internal security organization.

Given the nature of SSAC's work, it is reasonably foreseeable that SSAC may be required to deviate from its annual plan given developments in the space. We observe that SSAC activities are often driven by external events and believe SSAC should be free to deviate from the plan but also have accountability for deviations. SSAC should not be hamstrung by the annual plan but will be required to discuss deviations during the next planning cycle.

The reviewers note that much of the thought process and raw data for an annual planning process already exists informally today. The SSAC Executive Committee actively manages multiple projects on a relatively long-term calendar; we do not believe it a significant additional administrative burden to formalize the planning and reporting process; we note that the "work plan" document currently available on the SSAC web site, if kept up-to-date, is a good start.[39] Additionally, we believe the benefits to SSAC in terms of increased transparency, resourcing, and mission clarity are well worth the trade-off.

[39] ***The SSAC Work Plan Page.*** Internet Corporation for Assigned Names and Numbers, Security and Stability Advisory Committee. 1 April 2008. Accessed 12 February 2009. <http://www.icann.org/en/committees/security/ssac-workplan.htm>

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.

RECOMMENDATION 16: Implementation of an annual plan will reduce the need for frequent Executive Committee and full committee meetings. We recommend reducing meeting volume to: (a) Monthly Executive Committee meetings of 60 minutes or less in preparation for (b) Quarterly full SSAC meetings of three hours or less. We recommend SSAC continue to use project-oriented SSAC subgroups.

We observe that SSAC does not routinely publish meeting minutes; typically minutes are published only for SSAC meetings held in conjunction with ICANN meetings. Timely publication of meeting minutes is good governance practice for a board advisory committee and we recommend SSAC begin keeping and publishing minutes regularly. Minutes do not have to be detailed "transcripts" but rather simply keep a record of meeting time and date, attendees, and the topics discussed.

RECOMMENDATION 17: SSAC keep and publish meeting minutes on the SSAC web site in a timely fashion.

We note that, aside from the release of numbered work products, the SSAC web presence does not appear to be regularly updated. We believe an updated web presence would help keep individuals in the community informed as to the activities of SSAC and help maintain transparency.

RECOMMENDATION 18: SSAC should endeavor to keep their web site current to include work in progress and work planned for the future.

We believe that ICANN and SSAC would benefit from revisiting Task Area One of the existing SSAC charter to create a coordinated framework for considering security issues.

RECOMMENDATION 19: 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."

QUESTION: What is the right size for the SSAC?

While the objective of SSAC is to gather advice from a large pool of experts, the size of the SSAC has grown to greater than 30 and may be too large. Absent meeting minutes and formal metrics, it is difficult to objectively analyze the engagement level of individual members. In general, large volunteer groups tend to have few active contributors and many less active or non-contributors. Anecdotal evidence seems to indicate that this is the case with SSAC.

While a large volunteer committee is not in and of itself a problem, it makes it difficult to impose formal processes. The reviewers observe that regularly achieving a quorum with a committee this large would be difficult.

There is no requirement that all contributors to SSAC work products, presentations, or meetings are SSAC members. Because of this reality, and the flexibility granted to the Chair to invite guests to SSAC meetings as needed, we believe a dramatically smaller SSAC will be more manageable and productive. Additionally, a smaller SSAC will adapt more easily to an increased level of formality.

That being said, there are benefits of a larger committee, including broader geographic representation and availability of expertise.

QUESTION: Should SSAC membership have a geographic quotas?

SSAC is an advisory body chartered to provide the best advice possible to the Board. SSAC is not a representative body intended to represent stakeholders. As such, while geographic and cultural diversity are certainly positive factors, we do not advocate diversity for diversity's sake. We recommend the best experts be selected for SSAC membership regardless of their geographic proximity. As such, we do not recommend artificial geographic constraints on the SSAC membership.

RECOMMENDATION 20: SSAC should endeavor to find the best experts globally without regard for geographic proximity. SSAC membership should not be subject to artificial geographic quotas.

A large SSAC makes formal process, including achieving quorum and voting, more challenging. These challenges can be addressed through establishment of email based processes for voting and conducting business.

We recommend that the size of SSAC be reduced at the discretion of the chair to an approximate target of 15. The target of 15 is not a hard maximum; the Chair is free to operate SSAC at larger or smaller sizes as he or she sees fit. It is incumbent on the Chair to balance the need for a broad and diverse SSAC with the ability to conduct business effectively and efficiently.

RECOMMENDATION 21: The SSAC Chair establish a target size of 15 for SSAC membership; the Chair is free to operate SSAC at larger or smaller sizes as he or she see fit.

RECOMMENDATION 22: SSAC membership appointments be for a term of three years, renewable by the Board at the recommendation of the SSAC Chair indefinitely.

A three year term creates a built-in re-evaluation period for members without having to resort to asking for a resignation or removal. Effective SSAC members should be encouraged to participate for as long as they are willing, so we do not recommend term limits on SSAC members.

RECOMMENDATION 23: Do not impose term limits on SSAC members.

RECOMMENDATION 24: Stagger SSAC member terms such that roughly 1/3 of the terms are up for renewal each year.

The SSAC Board Liaison is appointed annually pursuant to the ICANN Bylaws. We believe occasional rotation of this position is important, so we recommend that the liaison not be permitted to serve more than three consecutive one year terms. Note that an individual is eligible for indefinite renewal as an SSAC member regardless of their role as a Board Liaison.

Should the Board terms be extended as recommended during the Board review process, and/or a Board risk committee is created, the term limits on SSAC Liaisons should be reevaluated as appropriate.

RECOMMENDATION 25: SSAC Board Liaison be permitted a maximum of three consecutive one year terms.

As a Board advisory committee, the Board controls the membership, largely pursuant to recommendations from the Chair. While the ICANN Bylaws are silent on the subject of removing individuals from advisory boards, we believe it appropriate to define the removal process in advance of an unfortunate situation where it becomes necessary.[40]

RECOMMENDATION 26: 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.

QUESTION: How should SSAC control the use of the SSAC brand?

As an indication of SSAC's success, the SSAC brand has become a visible, valuable, and respected brand. However, questions have arisen concerning the extent to which the SSAC brand is representative of all

[40] Given that the Bylaws are currently silent on this topic, the process is presently determined by California law.

SSAC members, a majority, a vocal minority, or individuals. This is exacerbated by the reality that no voting or formal rules of order are in use on SSAC making it impossible for outsiders to know how broadly consensus is reached. This has lead to a lack of comfort in certain areas of the community.

The reviewers observe that SSAC work products are almost certainly representative of the vast majority of the SSAC members due to the consultation and request for feedback process. However, we also observe that those outside of SSAC not familiar with its rather academic ways may hold a different perception. We therefore believe this issue requires proactive attention.

We believe that increased formality concerning the use of the SSAC brand is appropriate and will help further improve the standing of SSAC work products in the broader community. Managing the SSAC brand to assure it receives the continued respect in the space it has earned is a responsibility of the SSAC membership.

We believe managing the brand is twofold:

- A well-defined and transparent drafting, publication, and approval process
- A transparent mechanism for verifying support among SSAC members for a particular product

A published policy stating that the SSAC brand is only used on approved committee work products (i.e. those in the annual plan and related presentations), together with the annual planning process will address these items.

RECOMMENDATION 27: SSAC implement a policy explicitly stating that the SSAC brand (written or verbal) is to be used only on approved work products, and that use of the SSAC brand outside of these official products must be approved in advance by a majority vote of the SSAC.

We observe that a standing order of business during quarterly SSAC meetings will be reviewing and voting to approve work products - and thus formally approving the use of the SSAC brand providing a formal, defensible, and transparent mechanism.

RECOMMENDATION 28: SSAC formally and visibly adopt Roberts Rules of Order for conducting SSAC business meetings.

Formally adopting rules makes meetings more formal in appearance and in practice. At the same time, having a set of rules in place before they are needed is vastly preferred to the alternative.

QUESTION: How should SSAC deal with confidentiality?

SSAC currently has an unwritten policy of confidentiality. We recommend SSAC publish and post a written policy stating that the default SSAC confidentiality and privacy policy is Chatham House Rule (non attribution). Alternate policies are possible if necessary by mutual acknowledgement by all

involved participants. We believe a default policy of strict confidentiality is unnecessary, overly restrictive, and difficult to attain. We note that almost all SSAC communications occur over unsecured communications mechanisms, particularly email.

RECOMMENDATION 29: SSAC formally and visibly adopt Chatham House Rule as its default confidentiality policy. Other policies are used as necessary by mutual agreement.

5.4 Resourcing

As a part of the JAS engagement, we were specifically asked to determine whether SSAC was properly resourced. The question of whether SSAC is properly resourced begs the question: for what purpose and against what metrics? The reality is that since the current SSAC charter is sufficiently broad and SSAC is almost exclusively self-tasked, it is difficult to determine whether SSAC is meeting their obligations and is thus over or under resourced. For example, in 2008, SSAC released 12 work products; 4 more than the previous year. Is this the right number, too many, or too few? With no objectives to measure SSAC's performance against, the question of resourcing is ambiguous.

Many of our recommendations have focused on adding formality and structure to the SSAC such that a framework will exist in the future against which SSAC performance, resourcing, and efficiency can be evaluated. The annual plan - to include a work schedule and resource requirements - provides a mechanism for the ICANN Board to immediately and effectively address resource questions presented alongside a work plan.

RECOMMENDATION 30: Utilize the mechanisms recommended in this review, including the annual planning process, to regularly evaluate SSAC performance against objectives, resourcing, and efficiency metrics in the future.

5.5 Conflicts of Interest

The issue of perceived and actual conflicts of interest must be addressed with all boards and committees directly involved in or providing advice to a governance mechanism. We observe that while the SSAC Leadership does not appear to recognize this, perceived and actual conflicts as supposed by outsiders are a growing and at times debilitating concern. We observe that while SSAC members may feel that they are participating as individuals and "concerned citizens," outsiders may not see past their title and employer and assume that given corporate entities are "represented" on SSAC through these individuals.

JAS does not believe conflicts of interest have affected SSAC's past work in any way. However, there is a fairly pervasive perception in the community that conflicts of interest are a problem. Recognizing that "sunlight is the best disinfectant," we believe the issue can be put to rest fairly easily with three process improvements.

RECOMMENDATION 31: 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.

RECOMMENDATION 32: 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.

RECOMMENDATION 33: 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.

JAS believes that the recusals and dissents sections will be empty the vast majority of the time - which is in and of itself instructive and meaningful. We are mindful of potential politicalization of the SSAC and believe that this approach, as opposed to listing specific authors of each work product, will not lead to negative unintended consequences. Additionally, we do not believe the approach we have recommended will alter the legal ramifications of SSAC participation; however, each SSAC member is obligated to evaluate their own circumstances.

We note that ICANN has a conflicts of interest policy and we recommend that SSAC develop their own policy based on a subset of the ICANN policies.[41]

RECOMMENDATION 34: SSAC develop and post a conflicts of interest policy based on the ICANN Board policy.

Adoption of conflict of interest policies by charitable organizations is encouraged today by a many sources. In the United States, the Sarbanes-Oxley Act requires exchange-listed companies to adopt a conflicts policy, and the influence of that Act on nonprofit organizations has been substantial, particularly on large educational institutions and hospital foundations. Best practice codes recommend that charities adopt a conflicts policy. An advisory body comprised of outsiders having input into the governance process should certainly also have such a policy.

[41] ***Conflicts of Interest Policy.*** Internet Corporation for Assigned Names and Numbers. 04 March 1999. Accessed 14 February 2009. <http://www.icann.org/en/committees/coi/coi-policy-04mar99.htm>

6 Cross-Reference for Terms of Reference Questions

PART I. Does the SSAC have a continuing purpose in the ICANN structure?

Overall purpose

1. What security and stability issues has SSAC been dealing with and what issues should SSAC be dealing with or expecting to deal with given expected developments in the ICANN environment?	4.4 4.8 4.10
2. What purpose has the SSAC served? What should be the purpose of the SSAC in the future? Does the rationale for the SSAC in the Bylaws need to be revised?	4.1 5.1 5.2
3. Has SSAC activity accurately reflected the tasking and accountability set out in the Bylaws? Given the growth of ICANN since the original drafting of the Bylaws, what changes are needed to the SSAC component of the Bylaws to reflect the community's current needs?	4.1 4.8 5.1 5.2

Effectiveness

4. Has the SSAC been effective in delivering a security framework for Internet naming and address allocation services, as outlined in the Bylaws (see above)? What changes, if any, are required to make SSAC more effective?	4.4-4.10 5.1-5.5
5. Has the SSAC communicated effectively on security matters with the Internet technical community, as outlined in the Bylaws? What changes, if any, are required to make SSAC communicate more effectively?	4.4-4.10 5.1-5.5
6. Has the SSAC gathered and articulated requirements for security and stability to offer to those engaged in technical revision of the protocols and in operations planning? What changes, if any, are required?	4.4-4.10 5.1-5.5
7. How effective has the SSAC been in engaging in ongoing threat assessment and risk analysis, and advising the ICANN community accordingly? What changes, if any, are required?	4.4-4.10 5.1-5.5
8. How effective has the SSAC been in communicating with those with direct responsibility for Internet naming and address allocation security matters, and in synchronizing its advice with existing activities of those organizations? How effectively has SSAC communicated	4.4-4.10 5.1-5.5

with the ICANN technical community and operators and managers of critical DNS infrastructure? What changes, if any, are required?	
9. How effective has the SSAC been in its reporting to the Board on its activities and making policy recommendations to the Board? Has the SSAC been effective in providing advice to the ICANN Board on matters as outlined in the Bylaws? How effectively have SSAC recommendations been implemented? Does SSAC need to place greater effort on following through on recommendations that it makes? What changes, if any, are required?	4.4-4.10 5.1-5.5
10. How effective has the SSAC been in making policy recommendations to the ICANN community?	4.4-4.10 5.1-5.5
11. How does SSAC interact with other ICANN SOs and ACs? Are there regular communications between the SSAC and other SOs and ACs? How effective has the SSAC been in providing input and advice to other SOs and ACs? How effective has SSAC been in educating the ICANN community on security and stability issues? What changes, if any, are required?	4.4-4.10 5.1-5.5
12. Has SSAC played an appropriate role in ICANN policy development processes?	4.4-4.10 5.1-5.5
13. Does SSAC provide input to the ICANN budget process in a timely and effective manner to ensure that sufficient resources are allocated to security issues ? How effective is SSAC in engaging in the ICANN budget process? What input, if any, should SSAC have to ICANN's operations, corporate systems and plans?	4.4-4.10 5.1-5.5
14. Overall, how effectively has SSAC performed its role?	4.4-4.10 5.1-5.5

PART II. Is there any change in structure or operations that could improve the SSAC's effectiveness?

Structure and composition

15. What organizational structure, if any, is appropriate?	5.2-5.5
16. Given the security capabilities that exist in the ICANN community and in the broader Internet community, is a structure like SSAC still needed?	5.1-5.5
17. What is the optimal size of SSAC to maximize its effectiveness?	5.2-5.4
18. What should be the role of the Chair of the SSAC, and how should that person be	5.2-5.5

selected?	
19. Is the composition of SSAC appropriate for its mission? Does the current process for recruiting SSAC members meet SSAC's current and future needs?	5.2-5.5
20. Have members of SSAC had the skills needed to conduct their work effectively?	4.3-4.4 5.2-5.5
21. Does a non-voting liaison seat on the Board provide sufficient input and representation for SSAC? Is there any change needed?	5.2-5.5

Internal Operations and Procedures

22. How does the SSAC determine what advice to provide with respect to particular ICANN issues? What procedures govern how decisions regarding SSAC input for the Board and other ICANN entities are made? What are the benefits and costs of SSAC setting its own independent agenda as opposed to responding only to specific Board requests for advice? Are any changes needed to these procedures to improve the timeliness and quality of advice that is provided?	4.3 5.1-5.5
23. Do SSAC procedures allow it to maximize the expertise of committee members?	4.1-4.3 5.1-5.5
24. Given the volunteer nature of the committee, are the expectations placed on SSAC members appropriate? Should SSAC members be paid for their work?	5.2-5.4
25. Are sufficient safeguards in place to identify and address potential or actual conflicts of interest?	4.6 5.5
26. Does the SSAC operate in an accountable and transparent manner? Are any changes to SSAC procedures necessary to enhance accountability and transparency?	4.1 4.3 5.2-5.3
27. Are the SSAC's procedures sufficient to guide all aspects of its work?	4.3 5.3

Resources and support

28. Has the SSAC had the resources necessary to accomplish its tasks?	5.4
29. What kind of support has ICANN provided to the SSAC? What is the appropriate level of financial, institutional and staff support that should be provided to SSAC given expected	4.3

developments in the ICANN environment?	5.2-5.4

Overall

30. What other general or specific measures could enhance the effectiveness of SSAC?	1.1

7 Sources

(includes interviews scheduled after finalization of this section)

Name	F	P	E	W
Jaap Akkerhuis		•		•
Anonymous (n=8)			•	•
Raimundo Beca			•	
Les Bloom		•		
Doug Brent		•		•
Marilyn Cade		•	•	
Kimberly Claffy		•		•
Tim Cole	•			
John Crain		•		
Steve Crocker	••		••	•
Peter Dengate Thrush		•		
Kim Davies	•			
Barbara Fraser		•		
Roberto Gaetano	•			
Steve Goldstein				•
Chuck Gomes				•
Robert Guerra				•
Duncan Hart		•		
Jeremy Hitchcock				•

Name	F	P	E	W
Dennis Jennings	•			
Patrick Jones	•			•
Stacey King	•			
Peter Koch		•		•
Olaf Kolkman				•
Warren Kumari				•
Rick Lamb	•			
Matt Larson	•			
Paul Levins	•			
Denise Michel		•		•
Ram Mohan	•	•		•
Jonathon Nevett	•			
Nominet Corporation			•	
Olof Nordling	•			
Mike O'Connor				•
Dave Piscitello	•	•		
Rod Rasmussen				•
Greg Rattray	•	•		
Barbara Roseman		•		

Name	F	P	E	W
Kristina Rosette				•
John Schnizlein		•		•
Philip Sheppard		•		•
Paul Stahura	•			
Jean-Jacques Subrenat	•			
Bruce Tonkin				•
Paul Twomey	•	•		
Paul Vixie			•	
Dominic Weir	•			
David Ulevitch	•			
Liz Williams	•			
Suzanne Woolf	••			

Method Legend:
F – Face-to-face Interview
P – Phone Interview
E – Email Interview/feedback
W – Web survey feedback

Coding Legend:
• - Single dot represents a single instance
•• - Double dot represents multiple instances

8 CASE STUDY: SSAC activity in relation to VeriSign Site Finder

On September 15, 2003, VeriSign implemented the "Site Finder" service. Intended as a way to enhance the end-user experience of the Internet as well as provide business benefits to VeriSign, Site Finder changed the way that the COM and NET top level domains responded with presented with names for which no name server record exists.[42] Instead of returning the standard error code, it responded with the address of a VeriSign server which would handle both e-mail and web (HTTP) transactions. While strictly speaking, this change complied with the letter of published standards for the domain name system, there was a question as to the impact this service would have regarding given assumptions which are "deeply embedded in the behavior of Internet protocols and applications".[43] Many members of the Internet community[44] expressed concerns, some going so far as to call for the suspension or cessation of the Site Finder service.

On September 19, ICANN issued an advisory[45] requesting that VeriSign voluntarily suspend the Site Finder service and calling for input from SSAC regarding the security and stability impact. In a letter[46]dated September 21, VeriSign refused to honor ICANN's request.

SSAC issued a message to the ICANN board of directors on September 22[47] The SSAC message included a loose framework for the review of security and stability implications and scheduling a public meeting on October 7 to further establish the facts and determine the implications of the Site Finder service.

While the SSAC message contained some technical jargon and specialized terminology, it was very approachable for readers with a basic familiarity with the Internet's Domain Name System. More

---

[42] ***VeriSign's Site Finder Implementation***. VeriSign, Inc. 27 August 2003. Accessed 10 February 2009. <http://www.VeriSign.com/resources/gd/Site Finder/implementation.pdf>

[43] ***IAB Commentary: Architectural Concerns on the Use of DNS Wildcards***. Internet Architecture Board. 19 September 2003. Accessed 10 February 2009. <http://www.iab.org/documents/docs/2003-09-20-dns-wildcards.html>

[44] See http://www.icann.org/en/topics/wildcard-history.html for a list of many communiqués.

[45] ***Advisory Concerning VeriSign's Deployment of DNS Wildcard Service***. Internet Corporation for Assigned Names and Numbers. 19 September 2003. Accessed 10 February 2009. <http://www.icann.org/en/announcements/advisory-19sep03.htm>

[46] ***Letter from Russell Lewis (VeriSign) to Paul Twomey (ICANN)***. 21 September 2003. Accessed 10 February 2009. <http://www.icann.org/correspondence/lewis-to-twomey-21sep03.htm>

[47] ***Message from Security and Stability Advisory Committee to ICANN Board***. Internet Corporation for Assigned Names and Numbers, Security and Stability Advisory Committee. 22 September 2003. Accessed 10 February 2009. <http://www.icann.org/correspondence/secsac-to-board-22sep03.htm>

importantly, the clearly marked opinions and recommendations framed the discussion in a clear, technical context and provided actionable preliminary recommendations to the Board. Unfortunately, it was not a highly detailed message, which made it vulnerable to future criticism.

On October 3, 2003, several major actions took place. ICANN issued a second advisory[48] demanding the suspension of Site Finder relying on the September 22 SSAC message. ICANN's President and CEO also sent a letter to VeriSign[49]further articulating the demand to suspend Site Finder. Under the mounting public pressure and faced with ICANN's ultimatum, VeriSign suspended Site Finder.

In an October 3, 2003 letter, VeriSign laid out its initial claims as the basis for future legal action[50] In a separate letter to ICANN's general counsel[51]VeriSign critiqued the SSAC recommendations of 22 September, for a lack of "any data or facts on which to base the recommendation." In addition, they also raised concerns that the October 7 meeting would not be "objective, constructive, or fair" due to the format and restrictions placed on VeriSign's involvement. It also asked for formal documentation of SSAC processes and procedures and laid out a series of requests for ICANN's activity at and prior to the October 7 meeting. ICANN responded on October 6[52]discussing the SSAC process by which information would be gathered for their final recommendations.

---

[48] ***Advisory Concerning Demand to Remove VeriSign's Wildcard***. Internet Corporation for Assigned Names and Numbers. 3 October 2003. Accessed 10 February 2009. <http://www.icann.org/en/announcements/advisory-03oct03.htm>

[49] ***Letter from Paul Twomey (ICANN) to Russell Lewis (VeriSign)***. 3 October 2003. Accessed 10 February 2009. <http://www.icann.org/correspondence/twomey-to-lewis-03oct03.htm>

[50] ***Letter from Russell Lewis (VeriSign) to Paul Twomey (ICANN)***. 3 October 2003. Accessed 10 February 2009. <http://www.icann.org/correspondence/VeriSign-to-twomey-03oct03.pdf>

[51] ***Letter from James Ulam (VeriSign) to John Jeffrey (ICANN)***. 3 October 2003. Accessed 10 February 2009. <http://www.icann.org/correspondence/VeriSign-to-icann-03oct03-1.pdf>

[52] ***Letter from Paul Twomey (ICANN) to Russell Lewis (VeriSign)***. 6 October 2003. Accessed 10 February 2009. <http://www.icann.org/correspondence/twomey-to-VeriSign-06oct03.htm>

The October 7 meeting[53] and a second public meeting on October 15[54] allowed the community to investigate the security and stability impact of the Site Finder service. Both meetings included presentations from VeriSign justifying its service, as well as outside experts who were largely critical of the implementation of Site Finder.[55]

Following these meetings, SSAC issued its report[56] on July 9, 2004. Again, the report may have been more technical than could be readily digested by the general population, but the four recommendations were actionable to those who were familiar with ICANN's policy making processes and the underlying role of the DNS. VeriSign contested the report findings, analysis and recommendations[57], questioning: the process through which the report was generated; the constitution, legitimacy and scope of SSAC in relation to the scope of the report's findings and recommendations; procedural bias and exclusion of pro-VeriSign data in the course of SSAC's investigation; the possibility of conflict of interest between certain members of SSAC having real or perceived business interest in competition with VeriSign.

VeriSign alleged that SSAC had "prejudged" the Site Finder service in a manner "inconsistent with a dispassionate, technical assessment" and attributes a "desire to foment hysteria" to SSAC. VeriSign filed suit in Federal court in relation to the Site Finder incident on 26 February 2004; it is unclear how much of the criticism of the SSAC report was designed to integrate with the varied legal proceedings and how much of their analysis reflected actual (rather than alleged) shortcomings in the SSAC's processes, findings or recommendations.

---

[53] ***Agenda of Special Meeting to Gather Facts Relating to VeriSign's Change to the COM and NET Domains***. Internet Corporation for Assigned Names and Numbers, Security and Stability Advisory Committee. 7 October 2003. Accessed 10 Feb 2009. <http://web.archive.org/web/20040408204831/ssac.icann.org/agenda.htm>

[54] ***Agenda of Second Meeting to Gather Facts Relating to Queries of Uninstantiated Names in Top Level Domains***. 15 October 2003. Accessed 10 February 2009. <http://web.archive.org/web/20040408204536/ssac.icann.org/agenda-15oct03.htm>

[55] For detailed information about the presentations and positions of the speakers and discussions, please see the agendas (with links to the actual slide presentations) in footnotes 12 and 13, as well as the real-time captioning of both meetings at <http://web.archive.org/web/20040721010158/ssac.icann.org/captioning-07oct03.htm> and <http://web.archive.org/web/20040408205814/ssac.icann.org/captioning-15oct03.htm> (both links accessed 10 February 2009).

[56] ***Redirection in the COM and NET Domains***. Internet Corporation for Assigned Names and Numbers, Security and Stability Advisory Committee. 9 July 2004. Accessed 10 February 2009. <http://www.icann.org/committees/security/ssac-report-09jul04.pdf>

[57] ***VeriSign, Inc.'s Response to Report from the ICANN Security and Stability Committee re "Redirection in the COM and NET Domains."*** VeriSign, Inc. 5 August 2004. Accessed 10 February 2009. <http://www.icann.org/correspondence/verisign-response-ssac-05aug04.pdf>

SSAC's actions—which involved VeriSign, its competitors, and other interested parties, in part provided a technical defense for the ICANN demand that VeriSign suspend the Site Finder service. In addition, it underscores the essential need for ICANN's board of directors to obtain expert advice to support the security and stability of the Internet. While other parties and participants were involved in this incident, and their contributions have not been highlighted, it is clear that the SSAC played a pivotal role in the justification of the resolution to the Site Finder incident.