SSAC Activities Update

Rod Rasmussen, SSAC Chair | ICANN70 | March 2021

Agenda

1 SSAC Overview

2 SAC116: SSAC Comments on the SSR2 Review Team Final Report

3 SAC115: SSAC Report on an Interoperable Approach to Addressing Abuse Handling in the DNS

4 SAC114: SSAC Comments on the GNSO New gTLD Subsequent Procedures Draft Final Report

5 Updates on Name Collision Analysis Project and SSAC Current Work

6 SSAC Skills and Potential New Member Outreach

Security and Stability Advisory Committee (SSAC)

Who We Are

- ◎ **33** Members

- ◎ Appointed by the ICANN Board

What We Do

Role: Advise the ICANN community and Board on matters relating to the security and integrity of the Internet's naming and address allocation systems.

What is Our Expertise

- Addressing and Routing
- Domain Name System (DNS)
- DNS Security Extensions (DNSSEC)
- Domain Registry/Registrar Operations
- DNS Abuse & Cybercrime
- Internationalization (Domain Names and Data)
- Internet Service/Access Provider
- ICANN Policy and Operations

How We Advise
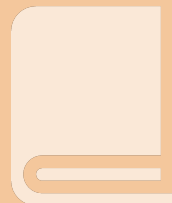
116 Publications since 2002

Security and Stability Advisory Committee (SSAC)

ICANN's Mission & Commitments

- Ensure the stable and secure operation of the Internet's unique identifier systems.

- Preserve and enhance the administration of the DNS and the operational stability, reliability, security, global interoperability, resilience, and openness of the DNS and the Internet.

SSAC Publication Process

Form Work Party → **Research and Write Report**

↓

Publish ← **Review and Approve**
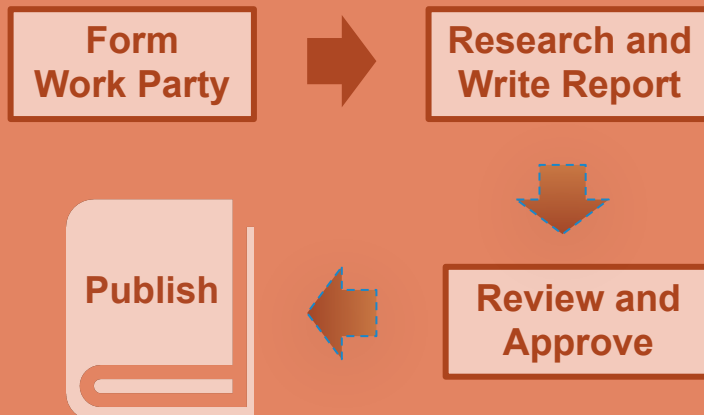
Consideration of SSAC Advice

(to the ICANN Board)

SSAC Submits Advice to ICANN Board

↓

Board Acknowledges & Studies the Advice

↓

Board Takes Formal Action on the Advice

1. Refer to GNSO for policy development

3. Direct Org to implement with public consultation

2. Forward to affected parties for their consideration

4. Decline advice with explanation

ICANN

Security and Stability Advisory Committee (SSAC)

Recent Publications

[SAC116]: SSAC Comments on the Second Security, Stability, and Resiliency (SSR2) Review Team Final Report

[SAC115]: SSAC Report on an Interoperable Approach to Addressing Abuse Handling in the DNS

[SAC114]: Comments on the GNSO New gTLD Subsequent Procedures Draft Final Report

ICANN|SSAC
Security and Stability Advisory Committee

Outreach

ssac.icann.org and SSAC Intro: www.icann.org/news/multimedia/621

www.facebook.com/pages/SSAC/432173130235645

SAC067 SSAC Advisory on Maintaining the Security and Stability of the IANA Functions Through the Stewardship Transition and SAC068 SSAC Report on the IANA Functions Contract: www.icann.org/news/multimedia/729

SAC116: SSAC Comments on the Second Security, Stability, and Resiliency (SSR2) Review Team Final Report

Geoff Huston

SAC116: Summary

- Endorses the fundamental conclusion behind the detailed SSR2 recommendations

- SSAC is of the view that issues of security and stability are of paramount importance in ICANN's role in the Internet's naming system

- SSAC is committed to supporting the efforts of the organization and community in responding

- SSAC appreciates the efforts made to ensure that SSR2 recommendations are metric-based with measurable performance indicators and to incorporate into them many SSR1 recommendations that lacked specificity

SAC116: Summary

- SSAC does however have a concern related to the capacity of the organization and community to implement these 24 comprehensive SSR2 recommendations in a meaningful and timely way

- The SSAC notes there are some items where the SSR2 Final Report appears to have taken a different stance from the SSAC's comments on the Draft Report but recognizes that legitimate differences in opinion on how to achieve a goal, informed by individual background and experience, do not necessarily imply lack of support for the goal

SAC115: SSAC Report on an Interoperable Approach to Addressing Abuse Handling in the DNS

Jeff Bedser

SAC 115: Summary

- SSAC proposes a general framework of best practices and processes to streamline reporting DNS abuse

- The SSAC Report covers the following topics:

  - Defining some aspects of the problem

  - Existing support mechanisms and resources

  - Primary point of responsibility for abuse resolution

  - Evidentiary terminology and standards

  - Escalation paths

  - Reasonable time frames for action

  - Availability and quality of contact information

  - A proposed path forward towards harmonizing efforts to address abuse incident reporting and handling

SAC 115: Findings

- Lack of coordination leads to inconsistent approaches to DNS abuse management

- An opportunity exists for the creation of a single entity [Common Abuse Response Facilitator] to independently convene, facilitate, guide, and provide clarity and predictability to all stakeholders in the greater DNS ecosystem

- A Common Abuse Response Facilitator would develop and implement a functional Internet-wide community model to directly confront the problem of Internet abuse, including DNS abuse

- ICANN has played similar roles in other initiatives that overlap with its mission and remit but extend into the wider Internet ecosystem:

  - Universal Acceptance Steering Group

  - ICANN DNS Symposiums

SAC 115: Recommendation

- Recommendation 1: The SSAC recommends that the ICANN community continue to work together with the extended DNS infrastructure community in an effort to

  - 1) Examine and refine the proposal for a Common Abuse Response Facilitator to be created to streamline abuse reporting and minimize abuse victimization; and

  - 2) Define the role and scope of work for the Common Abuse Response Facilitator, using SAC115 as an input.

- This community effort should include:

  - Domain registration providers that are part of the ICANN community.

  - Communities beyond the ICANN community, such as DNS infrastructure providers, content hosting providers, and the incident response community, and anti-abuse community

  - Other organizations that have worked on Internet abuse

- While the SSAC acknowledges the opportunity and need to create the anti-abuse efforts outlined in this report, it is not advocating for any particular organization or entity to fulfill them

SAC114: SSAC Comments on the GNSO New gTLD Subsequent Procedures Draft Final Report

Rod Rasmussen

SAC114: Summary

- SSAC directs its recommendations to the ICANN Board to consider along with the GNSO New gTLD Subsequent Procedures Final Report

- SSAC is concerned about proceeding with the delegation of new TLDs without addressing several fundamental issues related to the security and stability of the DNS

- SAC114 contains 7 recommendations:

  - Recommendations 1-3 address the SSAC's concerns regarding the potential impacts of additional delegations

  - Recommendations 4-7 specifically refer to elements of the Draft Final Report

SAC114: Recommendation 1

- **Recommendation 1**: The SSAC recommends that the ICANN Board initiate a fundamental review to determine whether continuing to increase the number of gTLDs is consistent with ICANN's strategic objective to "evolve the unique identifier systems in coordination and collaboration with relevant parties to continue to serve the needs of the global Internet user base." This review should be considered an input towards updating ICANN's strategic goals in conjunction with implementing the CCT Review Team's recommendations. Such a fundamental review should include at least the following areas of study based on prior rounds of the New gTLD program:

    - Impacts on root server operations

    - Impacts on SSR issues

    - Impacts on overall DNS operations

    - Analysis of how all metrics for success were met

    - Risk analysis

SAC114: Recommendations 2 and 3

- **Recommendation 2**: The SSAC recommends that, as part of the process for creating new gTLDs, ICANN develop and adopt a protocol for measuring progress against stated goals of the program and thresholds, which if crossed, may require mitigation actions. Such measurements and actions should consider the entirety of the DNS ecosystem.

- **Recommendation 3**: The SSAC recommends that the ICANN Board, prior to launching the next round of new gTLDs, commission a study of the causes of, responses to, and best practices for mitigation of the domain name abuse that proliferates in the new gTLDs from the 2012 round. This activity should be done in conjunction with implementing the CCT Review Team's relevant recommendations. The best practices should be incorporated into enforced requirements, as appropriate, for at least all future rounds.

SAC114: Recommendations 4-7

Recommendations 4-7 specifically refer to elements of the Draft Final Report:

- The ICANN Board should take the comments in SAC114 into consideration in the Board's deliberations

- ICANN org should develop reference materials or a set of tutorials to teach the basics of registry service provision as a prerequisite for new registry service providers

- Remove the words "intended use" as a defining characteristic to determine whether applications should be placed in the same contention set or not.

- The ICANN Board should consider the results of the Name Collision Analysis Project prior to authorizing the addition of new gTLDs

Name Collision Analysis Project

James Galvin, Patrik Fältström, Matthew Thomas (NCAP Co-Chairs)

Name Collision Analysis Project Update

- ICANN Board tasked SSAC to conduct studies to present data, analysis and points of view, and provide advice to the Board on name collisions

  - Specific advice regarding .home/.corp/.mail

  - General advice regarding name collisions going forward

- Studies to be conducted in a thorough and inclusive manner that includes other technical experts

  - 25 discussion group members, including 14 SSAC work party members

  - 23 community observers

Name Collision Analysis Project Update

- The original NCAP project consisted of 3 studies.

- Study 1 was principally a bibliography of all published work related to name collisions. It was completed in June 2020.

- Study 2 is principally the analysis of name collisions for the purpose of responding to the Board's questions and providing advice on how to evaluate future name collisions, including a root cause analysis of known name collisions.

- Study 3 will be a review of the effectiveness of current mitigation strategies and consideration of how to evaluate future mitigation strategies.

Name Collision Analysis Project Update

- As a result of work to date it was decided that Study 2 should be revised.

- A revised proposal has been submitted to the ICANN Board Technical Committee for review and, if approved, will ensure significant progress within the project.

- Revised outline describes the basic assumptions, major project elements, resources needed, and logistics of the project.

- Revised timeline is expected to start upon Board's approval and run 18 months.

- Revised budget reduces the overall cost by about 30%.

- Study 3 will be reviewed as Study 2 nears completion.

Updates on SSAC Current Work Parties

Current Work

- Name Collision Analysis Project

- SSR2 Review Team Final Report

- DNS Abuse

- Routing Security

- Root Service Early Warning System

- EPDP Phase 2a (Ongoing)

- SSAC Organizational Review Implementation

- Scan of Threats to Internet Naming and Addressing (Ongoing)

- Tracking SSAC Advice to the Board (Ongoing)

- DNSSEC and Security Workshops (Ongoing)

- Membership Committee (Ongoing)

Routing Security

- The scope is to examine the security and stability implications of insecurities in the Internet's routing system, and best ways network operators can address them
- The initial publication will generally explain
  - The Internet's routing system
  - Implications of incorrect route announcements
  - The role of network operators in securing the Internet's routing system
  - An indication of the size and urgency of routing security issues

Root Service Early Warning System

- The SSAC has chartered a work party to comment on OCTO-15: Recommendations for Early Warning for Root Zone Scaling and explore the possibility of a root service early warning system (EWS)
- This work party's tasks may include:
  - Reviewing all past material on the topic
  - Questioning the assumptions inherent in OCTO-15
  - Commenting on the feasibility, desirability, practicality and usefulness of a root service EWS
  - Investigating relevant data available for such a system and how such data might be made available to a future EWS
  - Reviewing developments in the DNS and root service, that could affect overall stability of the root service, including such developments as deployments of new technologies and changes to the overall DNS ecosystem

EPDP Phase 2A - Legal and Natural Persons

SSAC Work Party View:

- The distinction between legal and natural persons is an approximate proxy for whether data may be publicly disclosed
- Use explicit declarations and clear and explicit guidance
- Use a third status, "Unknown" to cover both existing registrations and new registrations where the answer is indeterminate
- Report on the number of Unknown registrations and gradually reduce the number
- Permit registrars to fold these requirements into their business process efficiently as long as the registrant is well informed and has appropriate choices
- All of the above is consistent with maximum disclosure and the expected use of differentiated access to support security research and other authorized uses

SSAC Organizational Review Implementation

- On 17 December 2018, the Independent Examiner (Analysis Group) published their Final Report on the 2nd SSAC Review
- On May 27, 2019, the SSAC published the Feasibility Assessment and Initial Implementation Plan (FAIIP) as SSAC2019-04
- On 12 March 2020, the SSAC's Detailed Implementation Plan based on the FAIIP was accepted by the Board
- Implementation updates were provided throughout 2020
- On 3 December 2020, the SSAC update stated that it considers that all recommendations approved by the Board have now been either completed, or integrated into ongoing SSAC processes, as documented in the SSAC Operational Procedures and proposed that implementation be recorded as complete.
- The 3 December SSAC Implementation Update (SSAC2020-13) was considered by the Board Operational Effectiveness Committee in January 2021 and is on the agenda for the March 2021 Board Meeting

Threats to Internet Naming and Addressing

- SSAC initiated an environmental scan of threats and risks to the DNS in the following categories:

    - DNS Security: Protocol, infrastructure, namespace

    - Domain Name Abuse

    - Addressing and Routing

    - Registration Services

- SSAC is using its threat identification, assessment, and ranking exercise to inform future work parties and membership recruitment efforts

- SSAC will be sharing its findings with the ICANN Board Technical Committee

Topics of Interest/Possible New Work

- Evolution of DNS Resolution

  - Alternative protocols

  - Resolverless DNS

  - Operational concentration of the DNS infrastructure

- DNSSEC DS key management and other registrar/registry control issues

- Concerns of overloading HTTPS for other privacy issues

- Examining datasets available from ICANN for use in the investigation of SSR-related issues that fall within SSAC's remit

- Examining practices that can potentially expose registrants to domain name hijacking via lame delegations

SSAC Skills and Potential New Member Outreach

Julie Hammer

SSAC Member Skills

- The skills of SSAC members span the following categories:

  - Domain Name System

  - Security

  - Abuse

  - Root Server System

  - IP Addressing/Routing

  - Registration Services

  - Internationalized Domain Names

  - Information Technology

  - Non-Technical (e.g., legal, risk management, business skills)

- The SSAC Skills Survey is used to document the skills of all existing and potential SSAC Members

SSAC New Member Outreach

- SSAC is looking for motivated professionals who have skills in the SSAC skills categories and, in particular, expertise or background in:
  - ISP operations
  - Large-scale measurement
  - Registrar Operations
  - Browser Development/Testing
  - Mobile Apps Development/Testing
  - Low bandwidth resource constrained Internet connectivity
  - Red Team experience
  - Risk management
  - Law Enforcement experience
- The SSAC is interested in increasing membership from Africa, Latin America, and Asia-Pacific

SSAC Contact for Potential New Members

- Individuals who are interested in enquiring about SSAC membership should:
  - Contact Rod or Julie,
  - Contact any member of SSAC Support Staff, or
  - Send an email to ssac-staff@icann.org

Questions to the Community

- What topics would you like SSAC to consider as work items?

- What would you like SSAC to comment on?

Thank you