ICANN 72
VIRTUAL ANNUAL GENERAL

SSAC Activities Update

Rod Rasmussen, SSAC Chair | ICANN72 | October 2021

Agenda

1

SSAC Overview

2

SAC117: Report on Root Service Early Warning Systems

3

SAC118: SSAC Comments on Initial Report of the EPDP on the Temporary Specification for gTLD Registration Data

4

SAC119: Feedback to the GNSO Transfer Policy Review PDP WG

5

Updates on Name Collision Analysis Project and SSAC Current Work

6

Q&A

Security and Stability Advisory Committee (SSAC)

Who We Are

- **36** 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

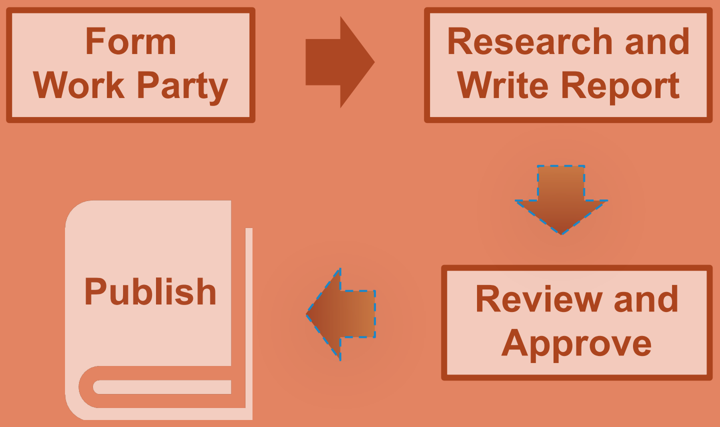
119 Publications since 2002

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

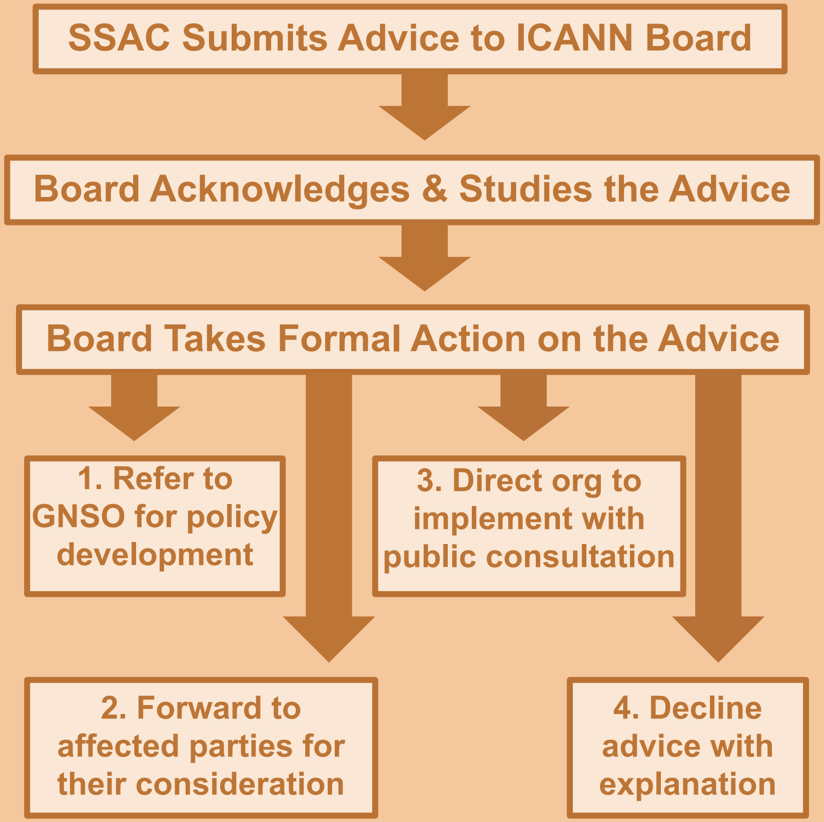
Research and Write Report

Review and Approve

Publish

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

2. Forward to affected parties for their consideration

3. Direct org to implement with public consultation

4. Decline advice with explanation

Security and Stability Advisory Committee (SSAC)

Recent Publications

[SAC119]: Feedback to the GNSO Transfer Policy Review PDP WG

[SAC118]: SSAC Comments on Initial Report of the Expedited Policy Development Process (EPDP) on the Temporary Specification for gTLD Registration Data Team – PHASE 2A

[SAC117]: Report on Root Service Early Warning Systems

ICANN | SSAC

Security and Stability Advisory Committee

Outreach

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

f 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

SAC117: Report on Root Service Early Warning Systems

Geoff Huston

SAC117: Summary

- SAC117 includes a brief summary of many relevant publications on the topic of Root Service Early Warning Systems.
- SSAC came to the conclusion that an early warning system for the root zone is currently infeasible, as was also concluded by OCTO-15.
- The root zone system is highly complex, and our current understanding of it does not allow us to predict imminent failure within its conventional and conservative operational parameters.
- This should not take away from efforts to better understand and gather data on the root server system, which root server operators are collecting, as described in RSSAC002 and RSSAC047.

SAC118: SSAC Comments on Initial Report of the Expedited Policy Development Process (EPDP) on the Temporary Specification for gTLD Registration Data Team – PHASE 2A

Steve Crocker

SAC118: Summary

- **EPDP-Temp Spec Phase 2A Topics**
  - Distinguishing Natural versus Legal Persons (9 questions)
  - Feasibility of Unique Contacts (2 questions)
- **SSAC Observations**
  - The System for Standardized Access/Disclosure (SSAD) is a new differentiated access system proposed to centrally handle requests for non-public registration data
  - There are three competing interests at work in the policy deliberations: privacy advocates, data requesters, and data controllers
  - SSAC believes it is very important for security investigators to get access to domain name registration data
  - A timely, reliable, effective, and efficient differentiated access system would make it possible to achieve a result that would be an improvement for all of the competing interests

SAC118: Recommendations

Recommendation 1: The Generic Name Supporting Organization (GNSO) and ICANN org should focus their attention on building and operating an effective differentiated access system.

Timely	It must come into operation soon.
Reliable	It must operate in a predictable and consistent fashion, both in the operation of the system and the decision-making by the participants of the system.
Useful	It must provide results that are of benefit to the requesters.
Efficient	It must provide responses to legitimate data requests quickly, and at a cost to all the parties that are acceptable for the purpose.
Easily Accessed	Gaining and maintaining credentials has to work well enough to facilitate—rather than impede—use.

SAC118: Recommendations

Recommendation 2: On Legal Versus Natural Persons

- A data element should be defined that denotes the legal status of the registrant.
- This data element should be displayed as part of the publicly available data.
- Registrants should be classified as either natural or legal persons. This should be required at the time of registration, for all new domain registrations. Registrars should be required to ask at relevant times whether the registrant is natural or legal.
- Registrants currently are able to and should continue to have the option of making their contact data publicly available. Legal person registrants should also have the ability to protect their data via privacy and proxy services.

SAC118: Recommendations

Recommendation 3: On Feasibility of Pseudonymous Email Contact

- The two policy objectives--namely (A1) the ability to quickly and effectively contact the registrant without disclosing personal data, and (A2) A common identifier that helps investigators to correlate registrations with common contacts should be considered separately.

- To achieve policy objective (A1), registrars should deploy (or continue to deploy) methods to support registrant-based email contact. The SSAC further recommends uniform requirements for safeguards be developed for the registrant-based email contact.

- To achieve policy objective (A2), additional research is needed on the methods, their efficacy, and their tradeoffs. We recommend the EPDP Phase 2A not specify a method for correlating registrations with a common contact at this time.

SAC119: Feedback to the GNSO Transfer Policy Review PDP WG

Steve Crocker

SAC119: Summary

- SSAC believes that it is important for registrants to experience a secure, stable, and smooth transition when transferring registrations between registrars.
- There are two specific security risks the SSAC highlighted:
  - A registrant's domain name is at risk of experiencing a discontinuity of DNS resolution, and when DNSSEC is in use, a discontinuity of validation, during a registration transfer if the transfer of DNS services is not considered during the process.
  - A registrant's domain name is at increased risk of being hijacked if the authInfo code is not managed according to best practice security principles.

Name Collision Analysis Project

James Galvin and Matthew Thomas
(NCAP Co-Chairs)

Name Collision Analysis Project

- 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
  - Co-chaired by James Galvin and Matt Thomas

NCAP: Our Work In Five Tasks

1. Root cause analysis
    a. In progress
2. Additional data collection
    a. Ongoing - coupled with Task 5
3. Answering board questions
    a. Ongoing - couple with Task 5
4. Case study of .corp, .home, .mail, .lan, .local, .internal
    a. **Draft in review**
5. Name collision analysis
    a. **Development of Analysis Workflow has begun**

NCAP: Critical Diagnostic Measurements

- Query Volume
- Query Origin Diversity
  - IP address distribution
  - ASN distribution
- Query TYPE Diversity
- Label Diversity
- Other characteristics
  - Open-Source Intelligence (OSINT)

- **Impact is determined by evaluating both Volume and Diversity across all CDMs**

Updates on SSAC Current Work Parties

Current Work Parties

- Name Collision Analysis Project
- Routing Security
- Reviewing Community Feedback on SAC114 [SubPro]
- Registration Transfer Policy Review (TPR)
- 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 provide a high level overview of
  - The Internet's routing system
  - Implications of incorrect route announcements
  - The role of network operators in securing the Internet's routing system
  - The size and urgency of routing security issues
- The initial focus is on the security and stability implications of routing incidents for the DNS and DNS operators

Reviewing Community Feedback on SAC114

- SSAC published SAC114: SSAC Comments on the GNSO New gTLD Subsequent Procedures Draft Final Report on 11 Feb 2021
- SAC114 contains commentary on both the final report of the GNSO Subsequent Procedures Working Group and observations and recommendations on wider issues tied to increasing the delegations of new gTLDs in the future.
- SSAC received feedback from the ICANN Board, RySG, and community members during ICANN70
- SSAC is actively considering the language and recommendations in SAC114 to update our advice informed by the feedback received from the community and shaped by an SSR perspective

Registration Transfer Policy Review (TPR)

- SSAC involvement via an invited subject matter expert
- Main focus of WG is consideration of authInfo code and loss of access to contact details
- We have raised the question of smooth transition of DNS operation, both signed and unsigned.

Topics of Interest/Possible New Work

- Evolution of DNS Resolution
  - Alternative protocols
  - Resolverless DNS
  - Operational concentration of the recursive and authoritative DNS infrastructure
- Examining datasets available from ICANN for use in the investigation of SSR-related issues that fall within SSAC's remit
- DNSSEC DS key management and other registrar/registry control issues
- Examining practices that can potentially expose registrants to domain name hijacking via lame delegations
- Technical implications of forced removal or transfer of a TLD

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 Rasmussen or Julie Hammer,
  - 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