SSAC Activities Update

Rod Rasmussen, SSAC Chair | ICANN68 | June 2020

Agenda

1

SSAC Overview

2

The Implications of DNS over HTTPS and DNS over TLS

3

SSAC Responses to Public Comment Opportunities

4

Update on Name Collision Analysis Project

5

Updates on SSAC Current Work Parties

6

SSAC Skills and Potential New Member Outreach

Security and Stability Advisory Committee (SSAC)

Who We Are

- **34** 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

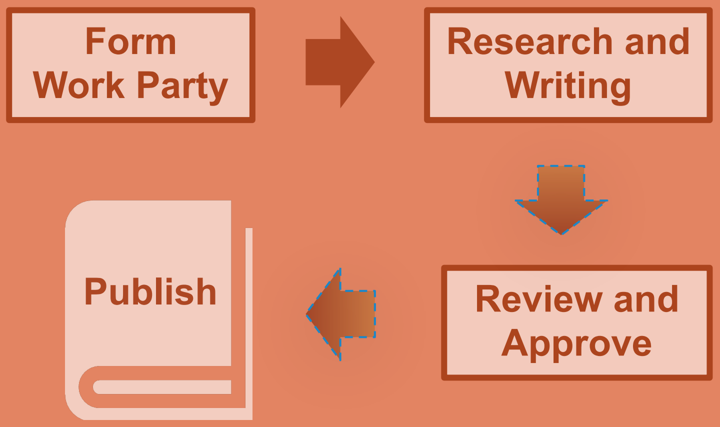
111 Publications since 2002

Security and Stability Advisory Committee (SSAC)

ICANN's Mission & Commitments

- To ensure the stable and secure operation of the Internet's unique identifier systems.
- Preserving and enhancing the operational stability, reliability, security and global interoperability, resilience, and openness of the DNS and the Internet.

SSAC Publication Process



Form Work Party

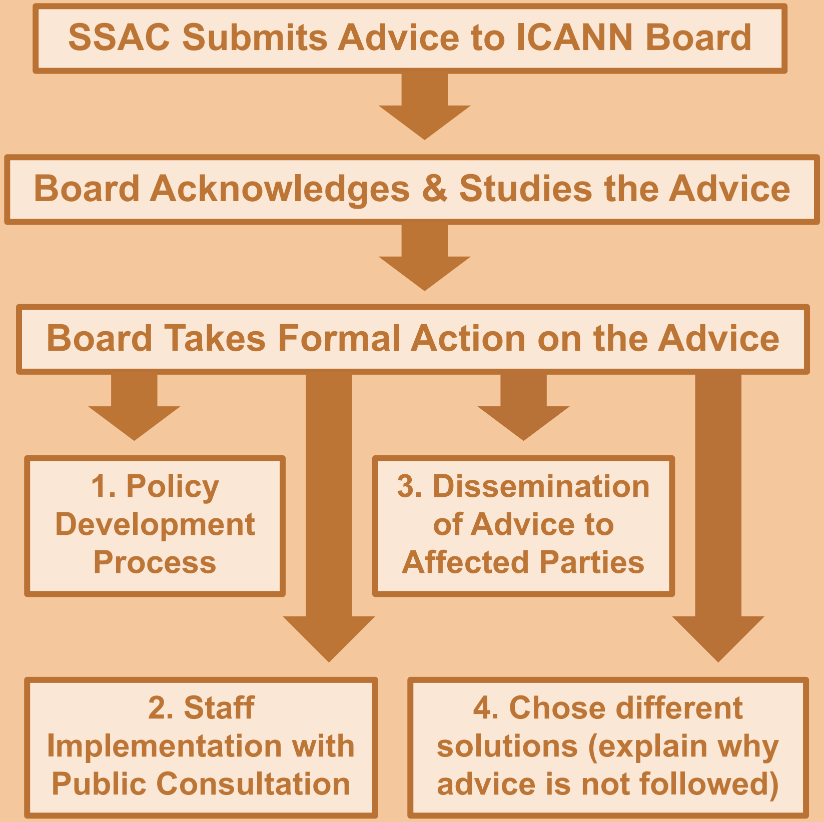
Research and Writing

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. Policy Development Process

2. Staff Implementation with Public Consultation

3. Dissemination of Advice to Affected Parties

4. Chose different solutions (explain why advice is not followed)

Security and Stability Advisory Committee (SSAC)

Recent Publications

[SAC111]: SSAC Comment on the Initial Report of the Temporary Specification for gTLD Registration Data Phase 2 Expedited Policy Development Process (4 May 2020)

[SAC110]: SSAC Comments on the Second Security, Stability, and Resiliency (SSR2) Review Team Draft Report (19 March 2020)

[SAC109]: The Implications of DNS over HTTPS and DNS over TLS (12 March 2020)

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

Current Work

- Name Collision Analysis Project
- Studying Abuse in the DNS
- SSAC Organizational Review Implementation
- Scan of Threats to Internet Naming and Addressing (Ongoing)
- DNSSEC and Security Workshops (Ongoing)
- EPDP Phase 2, Public Comment (Ongoing)
- Membership Committee (Ongoing)

Topics of Interest/Possible New Work

- Evolution of DNS Resolution
  - Alternative protocols
  - Resolverless DNS
  - Operational concentration of the DNS infrastructure
- Route hijackings and attacks on DNS infrastructure
  - Threats/risks, impacts, actions
- DNSSEC DS key management and other registrar/registry control issues
- Concerns of overloading HTTPS for other privacy issues

SAC109: The Implications of DNS over HTTPS and DNS over TLS

Barry Leiba & Suzanne Woolf

Implications of DNS over HTTPS and DNS over TLS

- The SSAC published SAC109 on 12 March 2020
- Explanation and comparison of DNS over HTTPS (DoH) and DNS over TLS (DoT), focusing on the standardization and deployment status
- Exploration of the effects on and perspectives of several different groups of stakeholders: parents, enterprise network managers, dissidents and protesters, and Internet service providers
- Examination of application resolver choice and what implications arise from these decisions
- Potential implications on the namespace due to DNS stub resolution moving to applications

What NOT to expect

- Declaration of universally agreed-upon “right” and “wrong” labels with respect to DoH and DoT, their implementation, and deployment choices
- Strong statements such as, “More privacy is always better,” or “More encryption is always better”
- Strong statements about trust models that we cannot all all agree with, because we all have different perspectives
- Recommendations to the ICANN Board

Conclusions

- Evaluations of DoH or DoT rely on the perspective of the evaluator based on the following questions:
  - How are they implemented
  - How they are deployed
  - What default settings are configured
  - Who uses them
- Regardless of perspective, the deployment of DoT and DoH will be disruptive, mainly in the implementation and deployment of the technology

Conclusions Continued

- Application-specific DNS resolution via DoH and DoT presents a host of challenges
  - How applications and operating systems work
  - How networks and endpoints work
  - Who has access to DNS query data
  - How to protect and manage networks in this new model

SSAC Responses to Public Comment Opportunities

SAC110: SSAC Comments on the Second Security, Stability, and Resiliency (SSR2) Review Team Draft Report

Geoff Huston

SSR2 Public Comment

- The SSAC focused its response to the SSR2 draft report on the 27 high-level recommendations and 108 component recommendations
- The SSAC is concerned about the large number of component recommendations contained in the draft report, and specifically their underlying rationale and their measurability
- Prioritization and consolidation of issues should be considered
- The report lacked an assessment of ICANN’s current status against SSR metrics which would help set a baseline
- In general, the outcomes sought by SSR2 for some recommendations are not clear

SAC111: SSAC Comment on the Initial Report of the Temporary Specification for gTLD Registration Data Phase 2 Expedited Policy Development Process

Ben Butler

Initial Phase 2 Report of the Temp Spec for gTLD Registration Data

- The SSAC considers it essential that the EPDP produce a policy framework that will deliver a continual improvement process for the System for Standardized Access/Disclosure (SSAD)
- The SSAC supports building a solid foundation that can be improved upon in a timely manner rather than holding out for an ideal system
- The Phase 2 Report currently falls short of what the SSAC believes is necessary and possible to address security and stability issues within ICANN’s remit
- To date, important in-charter issues involving the subject areas of natural-versus-legal persons, privacy/proxy service, and data accuracy are in danger of going unaddressed by the EPDP

SAC111: Recommendations to the EPDP Team and GNSO Council

- EPDP team should finish its deliberation on the policy framework for the continual improvement process for the SSAD and include it in the Phase 2 Final Report
- GNSO Council should direct the EPDP team to suspend work on financial sustainability. Text regarding it should be removed from the Phase 2 Final Report, and any work developed so far can be passed along to a follow-on policy working group’s charter.
- The GNSO Council should ensure that future PDPs stay entirely within the remit of their charters, regardless of the desire of a majority of participants to explore other areas. If such areas are identified by a PDP, then the charter must be modified and agreed to by participating groups prior to significant effort, time, and expense being applied to a non-charter area.

SAC111: Recommendations to the EPDP Team and GNSO Council

- The GNSO Council should consider the comments the SSAC has provided in Section 2 of this document in its deliberations on accepting the recommendations of the EPDP and any subsequent implementation of the approved recommendations.

Name Collision Analysis Project

James Galvin and Patrik Fältström

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
  - 24 discussion group members, including 13 SSAC work party members
  - 22 community observers

Name Collision Analysis Project Update

- **Study One: Gap Analysis**
  - Properly define name collision
  - Review and analyze past studies and work on name collision and perform a gap analysis
  - Study one draft report is currently out for Public Comment through 31 March 2020
- **Study Two: Root Cause and Impact Analysis**
  - Suggested criteria for determining whether an undelegated string should be considered a string that manifests name collisions, i.e., is a “collision string”
  - Suggested criteria for determining whether a Collision String should not be delegated
  - Suggested criteria for determining how to remove an undelegated string from the list of “Collision Strings” (aka mitigations)
- **Study Three: Analysis of Mitigation Options**
  - Identification and assessment of mitigation options
  - Production of recommendations regarding delegation

Name Collision Analysis Project Update

- July 2019: Definition of Name Collision and Scope of Inquiry for the NCAP posted for public comment through 20 August 2019
- July 2019: ICANN OCTO puts out RFP for contractor to perform bulk of Study One data gathering and analysis for input to the work party.
- October 2019: Vendor selected
- November 2019: Vendor began work on Study One
- February 2020: Draft report for Study One was put out for Public Comment through 31 March 2020
- May 2020: Proposed Final Report for Study One was put out for Public Comment through 17 June 2020
- **June 2020: The NCAP Discussion Group continues to meet to discuss questions from the ICANN Board and the shape of potential future studies/work**

Updates on SSAC Current Work Parties

DNS Abuse

- SSAC invited four external work party members from Donuts, Amazon, Cloudflare, and NCA
- SSAC will not provide a formal definition of “abuse” but will provide a framework for different parties to utilize in abuse handling and prioritization
- Work party is progressing on an escalation framework to mitigate abuse victimization
- Future study areas may include
    - Examination of successes and failures in dealing with abuse under current paradigms/policy
    - Study of effective anti-abuse practices by contracted parties

EPDP on the Temp. Spec. for gTLD Registration Data

- Work party to support SSAC members that are sitting on the EPDP WG
- Current SSAC Members on EPDP WG:
  - Tara Whalen
  - Ben Butler
  - Rod Rasmussen (Alternate)
  - Greg Aaron (Alternate)
- The SSAC participates to make sure the positions articulated by the past SSAC advisories are made available and represented in the ePDP work.

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
  - DNS Abuse
  - Addressing and Routing
  - Registration Services
- At its September 2019 workshop the SSAC held an exercise to assess each threat/risk and rank items by event probability and potential event impact
- SSAC is continuing its threat identification, assessment, and ranking exercise to inform future work parties and membership recruitment efforts

Private-Use TLDs

- The SSAC is currently considering TLDs available for private-use
- Currently, many enterprises and device vendors use locally-defined domain names to support their applications and infrastructure in the form of a name within a hierarchy rooted in a pseudo-TLD
- The SSAC is debating the merits of registering a Private-Use TLD to be used in a manner similar to the current use of private IP address space
- The SSAC is also debating the merits of adding the Private-Use TLD (if registered) to the root zone, and if so, what resource records to add

SSAC Skills and Potential New Member Outreach

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