



# SSAC Activities Update

Rod Rasmussen, SSAC Chair | ICANN67 | March 2020

# Agenda

---

1

SSAC  
Overview

2

The Implications of  
DNS over HTTPS and  
DNS over TLS

3

SSAC Responses to  
Public Comment  
Opportunities

4

Environmental Scan  
of Threats and Risks  
to the DNS

5

Update on Name  
Collision Analysis  
Project

6

Updates on SSAC  
Current Work Parties

# Security and Stability Advisory Committee (SSAC)

## Who We Are



- **34 Members**



- Appointed by the ICANN Board

## What We Do

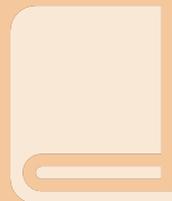


Role: Advise the ICANN community and Board on matters relating to the security and integrity of the Internet's naming and address allocation systems.

## 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



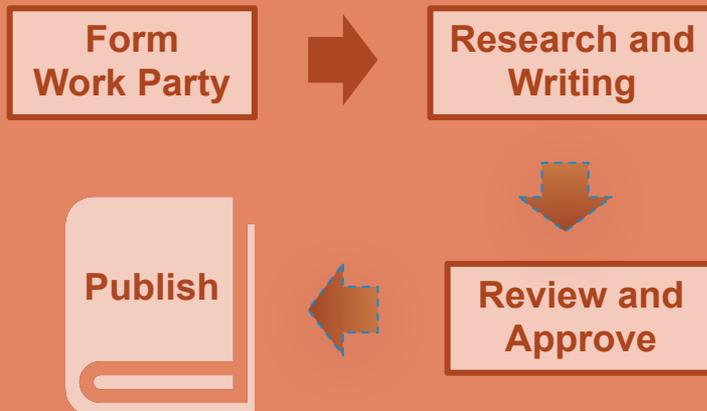
**108 Publications  
since 2002**

# 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



## 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

3. Dissemination of Advice to Affected Parties

2. Staff Implementation with Public Consultation

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

# Security and Stability Advisory Committee (SSAC)

## Recent Publications

[SAC108]: SSAC Comments on the IANA Proposal for Future Root Zone KSK Rollovers (29 January 2020)

[SAC107]: SSAC Comment to NIST on Quantum Cryptography Algorithms (3 December 2019)

**ICANN | SSAC**  
Security and Stability Advisory Committee

## Outreach



ssac.icann.org and SSAC Intro:  
[www.icann.org/news/multimedia/621](http://www.icann.org/news/multimedia/621)



[www.facebook.com/pages/SSAC/432173130235645](https://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](http://www.icann.org/news/multimedia/729)

# Current Work

---

- SSR2 Public Comment
- Name Collision Analysis Project
- SSAC Organizational Review Implementation
- Studying Abuse in the DNS
- 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

---

- DNSSEC DS key management and other registrar/registry control issues
- Domain name hijacking attacks
- .internal
- Resolverless DNS
- Operational concentration of the DNS infrastructure
- Concerns of overloading HTTPS for other privacy issues

# 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 will be publishing a report on this topic in the near future
- 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 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

- 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

# SAC108: SSAC Comments on the IANA Proposal for Future Root Zone KSK Rollovers

Jacques Latour

- SSAC has previously commented on root zone KSK rollovers in SAC063, SAC073 and SAC102
- In general, the SSAC believes the report is an adequate high-level plan and that further delay in planning for subsequent KSK rollovers is not merited.
- Raises minor concerns with IANA's Proposal for Root Zone KSK Rollovers and requests further detail from IANA on numerous items.
- The SSAC expects IANA to produce a more detailed final plan for public consultation prior to rolling the KSK again.

# SSAC2020-06: SSAC Public Comment on the Initial Report of the New gTLD Auction Proceeds Cross-Community Working Group

John Levine

# Initial Report of the New gTLD Auction Proceeds CCWG

---

- The SSAC does not object to any of the 12 recommendations in the report
- The SSAC supports the finalization of this report following the Public Comment period so that the work of the CCWG can be concluded.

**Recommendation:** The SSAC recommends that, following the completion and submission of the CCWG's report, the next step in the process be to have an outside expert with a demonstrated track-record in designing funding programs review the report, comment on its findings and recommendations, and use it as a basis to inform the Board on the design of a grant making process for the auction proceeds that implements grant making best practices.

# Initial Report of the New gTLD Auction Proceeds CCWG

---

- There are process issues that have negatively impacted community-wide reviews and cross-community working groups.
  - The length of time taken for the CCWG to conduct its work is regrettable
  - Other issues of concern are volunteer burn-out, ICANN Org overload, and recommendations that are not crisp and actionable.
- The SSAC will incorporate further details and examples of the issues identified in this particular CCWG in future comments on ICANN cross-community efforts

# SSAC2020-05: SSAC Public Comment on Third Accountability and Transparency Review Team (ATRRT3) Draft Report

Julie Hammer

# ATRT3 General Comments

---

- Volunteer overload and burnout
  - The workload on community members has significantly increased in recent years
  - All potential recommendations should be carefully assessed for absolute necessity, practicality and cost effectiveness before being proposed
  - Realistically, only fewer reviews and CCWGs will reduce this burden on volunteers
- ICANN Org overload
  - The large number of reviews and CCWGs - and the lack of prioritization for their recommendations - has led to an intractable workload for ICANN Org

# ATRT3 Specific Comments

---

- The SSAC is greatly concerned by the large disparity between ICANN's self-assessment of implementation of ATRT2 recommendations and the assessments of the review team
- The SSAC supports a community-led process for prioritising the recommendations of Specific Reviews on an annual basis but not exactly as proposed by the ATRT3. The SSAC prefers that:
  - The SO/AC Leadership should develop the ongoing prioritization framework and process, aligned to the Strategic Plan, which would then be subject to community consultation before finalization
  - The SO/AC Leadership, facilitated by ICANN Org, should lead the annual process to prioritize the FY Operating Plan and Budget, encompassing the recommendations of Specific Reviews. The FY Operating Plan and Budget would then, as currently occurs, be subject to community consultation and adjustment based on feedback.

# ATRT3 Specific Comments

---

- The SSAC has mixed views on the introduction of an Independent Accountability Office (IAO) and sought a more detailed proposal from ATRT3 regarding how an IAO would function.
- The SSAC does not support the conduct of Organizational Reviews as 3-5 day workshops focussed on self-inspection but suggested scheduling flexibility be incorporated into the Bylaws to enable an approach that avoids volunteer burnout and ICANN Org overload
- The SSAC considers there is merit in seeking to combine the scope of some of the Specific Reviews and even considering very seriously whether some aspects of these reviews are required at all.
- The SSAC considers that an external appropriately skilled consultant should be engaged to conduct the SSR2 Review, supports the extension of the timeline between external reviews to approximately 7 years and recommends that scheduling flexibility be incorporated into the Bylaws to enable an approach that avoids budget stress and volunteer burnout.

# ATRT3 Specific Comments

---

- These comments are consistent with comments previously provided by the SSAC on options to improve Specific and Organizational Reviews:
  - SSAC2018-18: SSAC Comment on Short-Term Options to Adjust the Timeline for Specific Reviews dated 24 July 2018
  - SSAC2018-19: SSAC Comment on Long-Term Options to Adjust the Timeline of Reviews dated 24 July 2018

# SAC107: SSAC Comment to NIST on Quantum Cryptography Algorithms

John Levine

# SAC107: Comments to NIST on Quantum Crypto

---

- Feedback in response to National Institute of Standards (NIST)'s post-quantum cryptography second-round candidate algorithms.
- NIST is in the process of standardizing post-quantum cryptographic algorithms.
- Focuses on the role that new cryptographic algorithms would have in the implementation of DNSSEC.
- The SSAC is concerned that some of the candidate algorithms have very large keys, and the impact these large keys would have on DNSSEC. For example, some of them are too large to encapsulate in DNS messages.

# Scan of Threats to Internet Naming and Addressing

Rod Rasmussen

# 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

# 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
  - Appointed Matt Thomas as Co-Chair from the community

# 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 Name Collision Analysis Project 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 begins work on Study One
- **February 2020: Draft report for Study One is out for Public Comment through 31 March 2020**

# Updates on SSAC Current Work 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.
- The WP is drafting a public comment response on the EPDP phase 2 initial report for SSAC review

# DNS Abuse

---

- SSAC invited four external work party members from Donuts, Amazon, Cloudflare, and NCA
- Work party recently formed
- Several potential areas to study/comment upon
- SSAC will not provide a formal definition of “abuse” but will look to provide a roadmap for handling abuse across various DNS parties
- 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

# SSR2 Public Comment Work Party

---

- The SSAC is focusing 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
- The outcomes sought by SSR2 for some recommendations are not clear
- The SSAC intends to prepare a separate document commenting on the cross community review processes

# 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