ICANN 76
COMMUNITY FORUM
CANCÚN
11-16 March 2023

SSAC Activities Update
March 2023

Agenda

- SSAC Overview
- Recent SSAC Correspondence
- Name Collision Analysis Project
- SSAC Work Parties
- Tracking ICANN Top Priorities
- SSAC New Member Outreach
- Q&A

Security and Stability Advisory Committee (SSAC)

Who We Are

- **35** 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

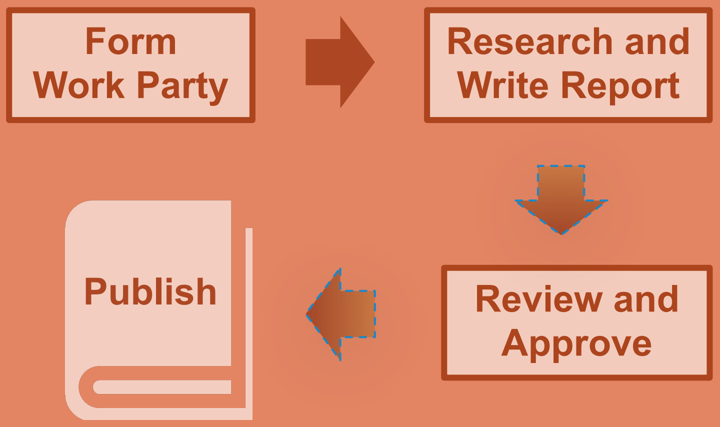
121 Publications since 2002

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

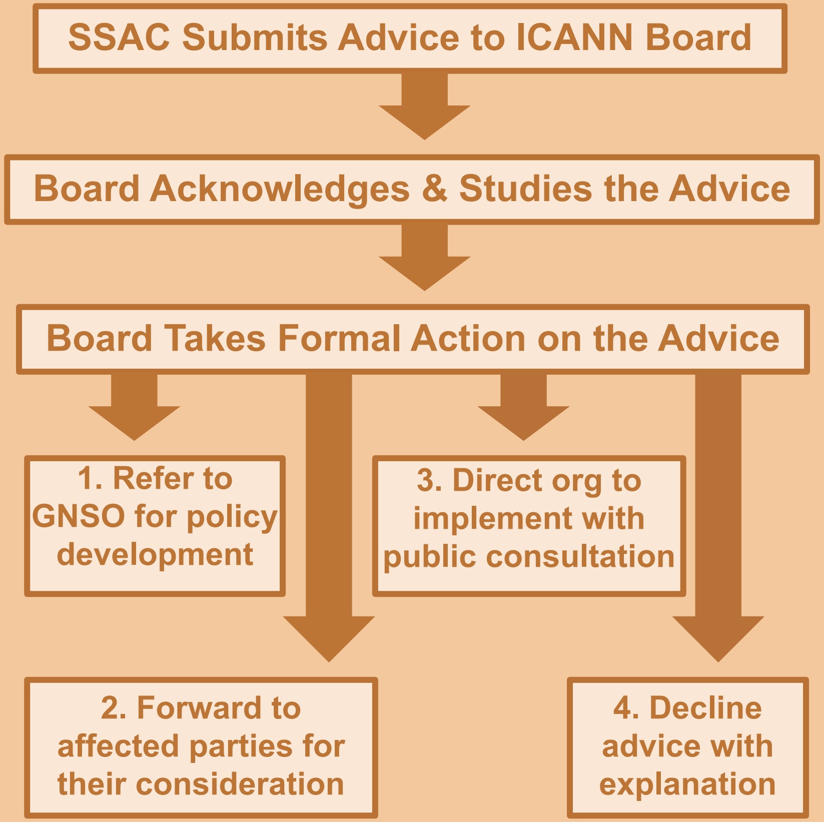
Research and Write Report

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

[SAC121]: SSAC Briefing on Routing Security

[SAC120]: SSAC Input to GNSO IDN EPDP on Internationalized Domain Name Variants

Addendum to SAC114: Additional Context for Recommendation 1, Recommendation 3, Recommendation 7, and Additional References

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

Recent SSAC Correspondence

Rod Rasmussen

SSAC2023-02: SSAC Public Comment on Proposed Procedure for Selecting a Top-Level Domain String for Private Use

- Response to ICANN org's proposal to implement the recommendation from SAC113: SSAC Advisory on Private-Use TLDs
- SSAC's comments:
    - The proposed procedure needs to have more detail in it, especially about how it will assess Criteria 3 and 4.
    - This document already states that both these criteria are subjective, but makes no proposal about how judgements will be made.
    - The proposed procedure should explain how candidate strings will be tested for confusing similarity, memorability, and meaningfulness, taking into account both native and non-native speakers of the language(s) in which the string is intended to be understood.

SSAC2022-12: SSAC Public Comment on Proposed Amendments to the Base gTLD RA and RAA to Add RDAP Contract Obligations

- Comment 1: On the topic of reporting requests for domain registration data
  - Proposed language permits an operator of multiple TLDs to allocate counts of queries to individual TLDs in an inaccurate manner, as long as the sum of all counts equals the total queries for the operator
  - This is an improvement but it potentially serves to normalize the creation of inaccurate reports
- Comment 2: On the topic of the sunsetting of web-based WHOIS services:
  - Potential negative ramifications of sunsetting web-based WHOIS services for end users as native RDAP output is not typically easily human-readable
  - Good for contracted parties to be aware so they can serve their customers
  - Good for third parties creating RDAP lookup tools to be mindful of implementing rate limits

SSAC2022-11: SSAC Public Comment on Draft Terms of Reference for the Holistic Review Pilot

- SSAC provides specific feedback to improve clarity in the draft Terms of Reference
- SSAC also provides more in depth comments regarding the Holistic Review Pilot:
    - It seems unlikely that this Pilot Holistic Review could completed within the 18 month timeframe when the additional task of developing and documenting procedures must be undertaken
    - Terms of Reference should make very clear what the scope of the Holistic Review is and any disagreement on the documented scope should be highlighted and resolved through the Public Comment Process.
    - Mission of the review would be improved by a minor expansion of the scope to consider if there are any interests not currently represented within the current ICANN structures

Name Collision Analysis Project

Matt Thomas and Suzanne Woolf (Co-Chairs)

NCAP Background

- 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
  - Chaired by Matt Thomas and Suzanne Woolf

NCAP - Recent Publications

- Case Study of Collision Strings
  - Studies of .corp, .home, .mail, .internal, .lan, and .local using DNS query data from A and J root servers.
  - Highlight changes over time of the properties of DNS queries and traffic alterations as a result of DNS evolution.
- A Perspective Study of DNS Queries for Nonexistent Top-Level Domains
  - Aims to understand the distribution of DNS name collision traffic throughout the DNS hierarchy
  - Provide insights into where and how DNS data can be collected and assessed.

NCAP - Key Findings so far

- Name collisions are and will continue to be an increasingly difficult problem; case study indicates impact has increased
    - DNS service discovery protocols and suffix search lists are a continuing problem
- Critical diagnostic measurements (CDMs) are defined as a way to measure name collisions by informing the assessment of the risk of delegation
- Mitigation and remediation is problematic, increasingly difficult as the volume and diversity of CDMs increases
- Designation of a TLD for private use (as advised by SSAC in SAC113) can mitigate the risk over the long term, but not immediately
- Existing measurement platforms could be extended to help inform applicants

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)

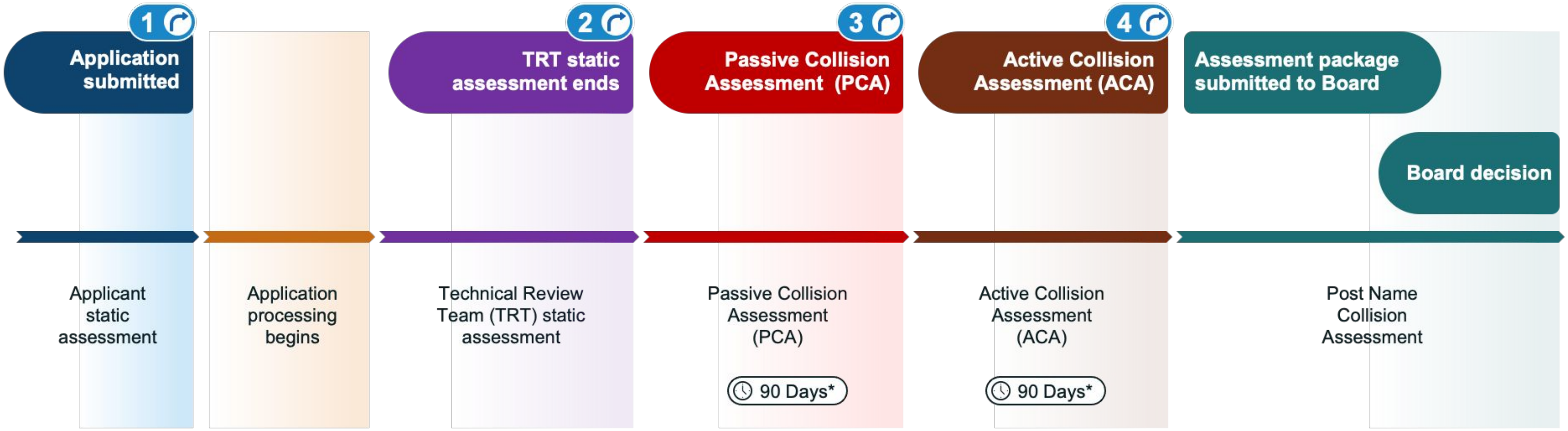
- **Impact (or Harm) is determined by evaluating both Volume and Diversity across all CDMs**

NCAP - Workflow Goals

- To ensure that name collisions can be assessed
  - Requires name collisions to be visible, if they exist

- To ensure there is an opportunity for a mitigation or remediation plan to be developed and assessed
  - Requires understanding the cause of name collisions such that a mitigation or remediation plan (or both) can be developed and assessed

NCAP - Workflow and Timeline



1 Application submitted

Applicant static assessment

Application processing begins

2 TRT static assessment ends

Technical Review Team (TRT) static assessment

3 Passive Collision Assessment (PCA)

Passive Collision Assessment (PCA)

90 Days*

4 Active Collision Assessment (ACA)

Active Collision Assessment (ACA)

90 Days*

Assessment package submitted to Board

Board decision

Post Name Collision Assessment

Offramp Options

1 – Applicant decision only

2,3, & 4 – TRT identifies risk in its written report; notifies Board and Applicant who consider mitigation, remediation, or withdrawal; OR no risk concerns and assessment proceeds to next step

*: 90 days of data collection followed by time for report and decision

NCAP - Workflow and Technical Review Team

- Need to be independent and neutral experts
- Technical expertise must include:
  - Knowledge and understanding of DNS specifications, provisioning, and operation
  - Knowledge and understanding of Internet infrastructure
    - Where it intersects with the DNS
    - Where it intersects with the usage of the DNS by applications and services
  - Ability to review and understand data collected (e.g., CDMs)
  - Ability to understand and assess risk
- Four responsibilities
  - Assess the visibility of name collisions
  - Document data, findings, and recommendation(s)
  - Assess mitigation and remediation plan
  - Emergency response

NCAP - Workflow and Neutral Service Provider

- Responsible for operation of the servers that will collect the CDMs
  - Data privacy concerns are still under discussion
  - Is this part of the Technical Review Team or a separate team?
  - If a separate team, could there be more than one?

- Four responsibilities
  - Operate Passive Collision Assessment environment
  - Operate Active Collision Assessment environment
  - Log processing and analysis preparation for TRT
  - Emergency response

NCAP - How to Participate

- Join the discussion group
  - https://docs.google.com/forms/d/1PDIX6sMIdP4vLn1LLuefxsup78mLM0iDb8ybWhlw2T4/edit

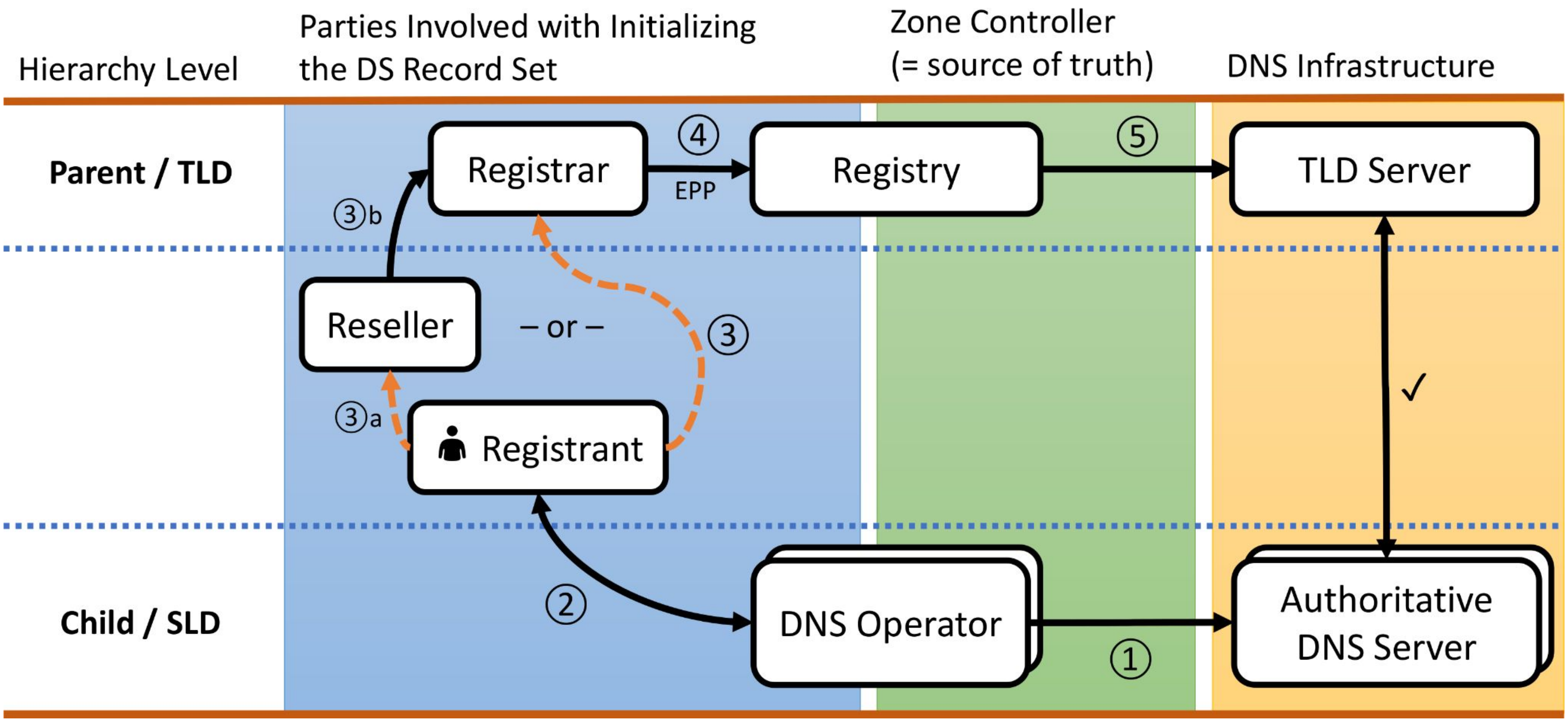
- Study 2 report nearing completion
  - Findings and Recommendations still in progress
  - Target is Public Comment before ICANN77

Updates on SSAC Work Parties

Current Work Parties

- Name Collision Analysis Project
- DS Automation
- Evolution of DNS Resolution
- Registrar NS Management
- DNSSEC and Security Workshops (Ongoing)
- Membership Committee (Ongoing)

DS Automation - Current Process



DS Automation - Considerations (1)

1. When the DNS Operator is not the same entity as the Registrar, the customary DS provisioning method is onerous and error-prone. It is perceived as frustrating and difficult, and not completed by 40% of Registrants.[1] This has become one of the choke points for DNSSEC adoption.

2. For many TLDs, DNSSEC operation is not automated from the Registrant's point of view, even though pieces of the infrastructure are. This is contrary to Registrants' expectations.

3. Recent protocol developments[2] created new mechanisms for automating the DS provisioning multi-party process, using signaling records published by the DNS Operator and consumed by the parent. The mechanism has working production implementations by several ccTLDs and Registrars.[3]

[1] Source: https://conferences.sigcomm.org/imc/2017/papers/imc17-final53.pdf

[2] RFC 7344, RFC 8078, draft-ietf-dnsop-dnssec-bootstrapping

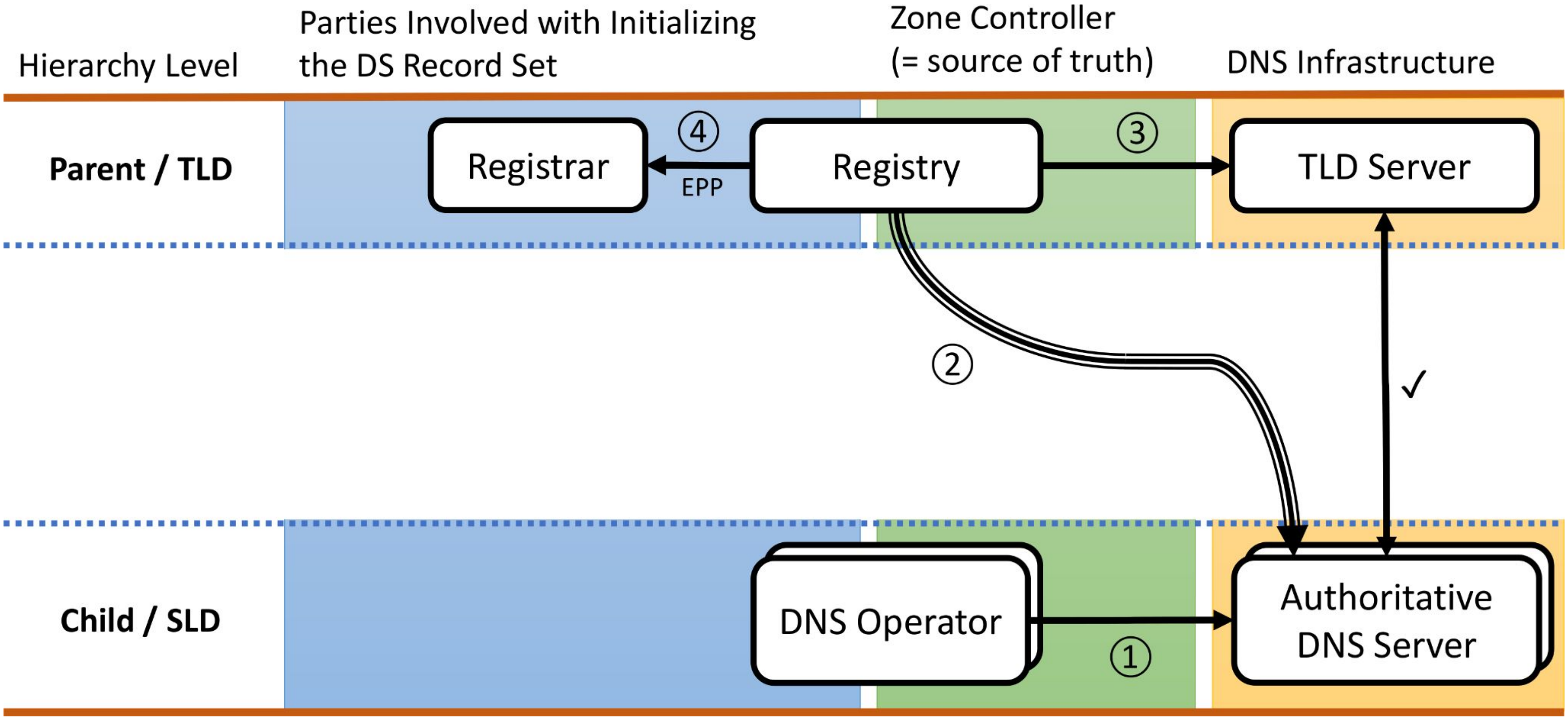
[3] https://github.com/oskar456/cds-updates

DS Automation - Considerations (1)

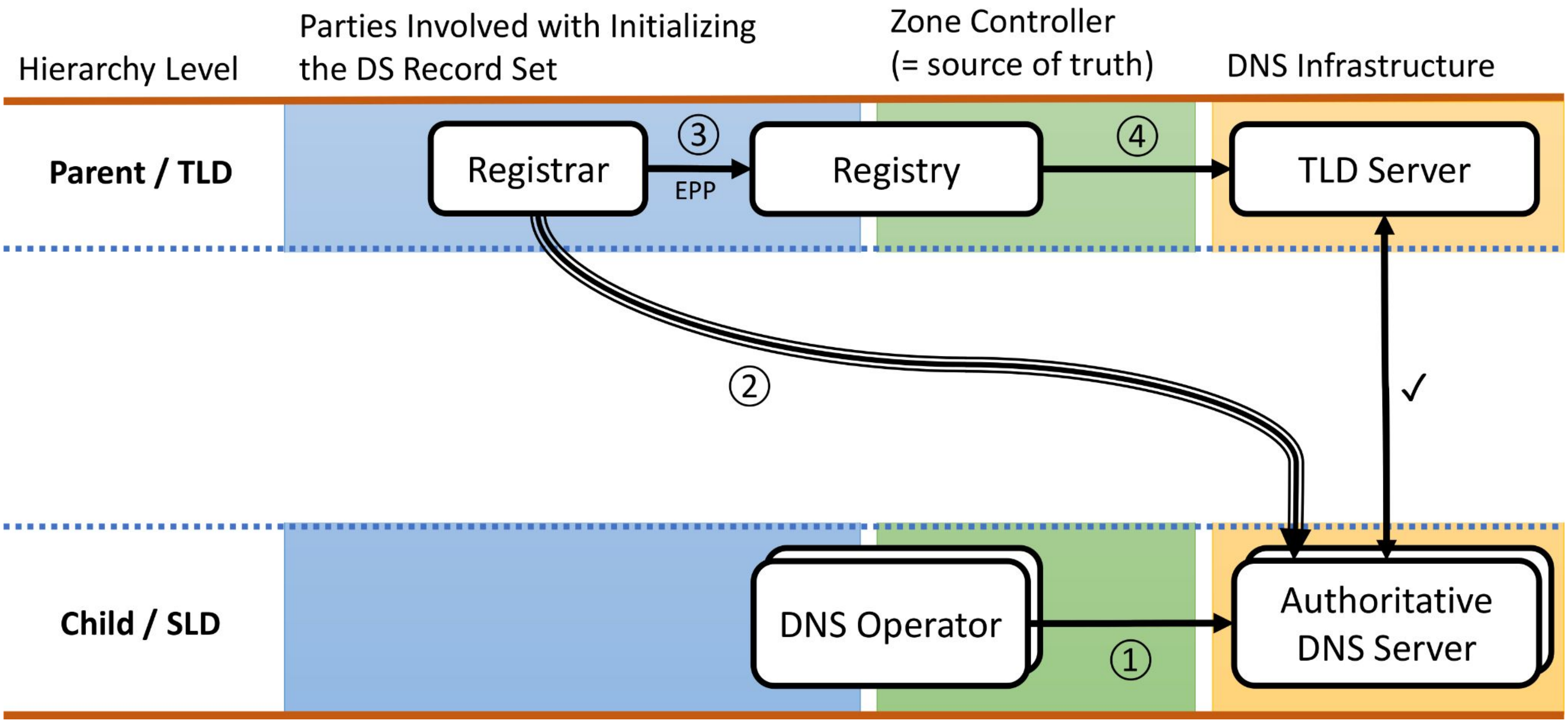
4. Enabling support for automatic acceptance of DS parameters directly from the Child DNS Operator requires the Registry/Registrar to make a number of technical decisions. These aspects are not show-stoppers, but answering them is a precondition for deployment.

The Work Party has asked ICANN Org for clarifications in the context of DS automation, which were received last week. The Work Party is now finalizing its findings, taking these answers into account.

DS Automation - Model 1



DS Automation - Model 2



Evolution of DNS Resolution Work Party

- **Goal:** Discuss technologies that are changing the nature of DNS resolution and the implications of these changes on the DNS namespace, provisioners, and operators of DNS infrastructure
- **Scope:** Explore the current state and evolving nature of DNS resolution with a focus on SSR issues related to alternative naming technologies (e.g., blockchain)
- **Deliverable:** An SSAC report that analyzes the effects of relevant new technologies. The report may also suggest methods to measure the implications of these technologies, and possibly propose instrumentation to provide measurements where there may be instrumentation gaps.
- **Intended Audience:** The ICANN community as a whole, including network operators, DNS software implementers, policy makers, and concerned Internet users.

Evolution of DNS Resolution - Preliminary Findings (1)

- Lots of software uses names that are syntactically compatible with the domain namespace. This makes this form of name pervasive.
- Names that are syntactically equivalent to DNS names are being used in alternate protocols and different contexts. This is partly because applications written for DNS names are easily modified to support syntactically equivalent names, and also because users are already comfortable with this naming syntax.
- Relatively few users understand that a top-level domain can sometimes signal an alternate protocol. For example, many Tor users know that .ONION designates the Tor protocol. However, very few users are aware of all of the special top-level domain names, and surely more will come over time.

Evolution of DNS Resolution - Preliminary Findings (2)

- Alternate protocols are increasingly using domain names that may collide with domain names in use, now or in the future. Regardless of the resolution mechanism used.
- There is currently no mechanism or procedure at ICANN, the IETF, or other institution that can facilitate coordinated use of the domain namespace for multiple protocols. It would be good to establish such a voluntary mechanism for those who would find it helpful.

Registrar NS Management Work Party

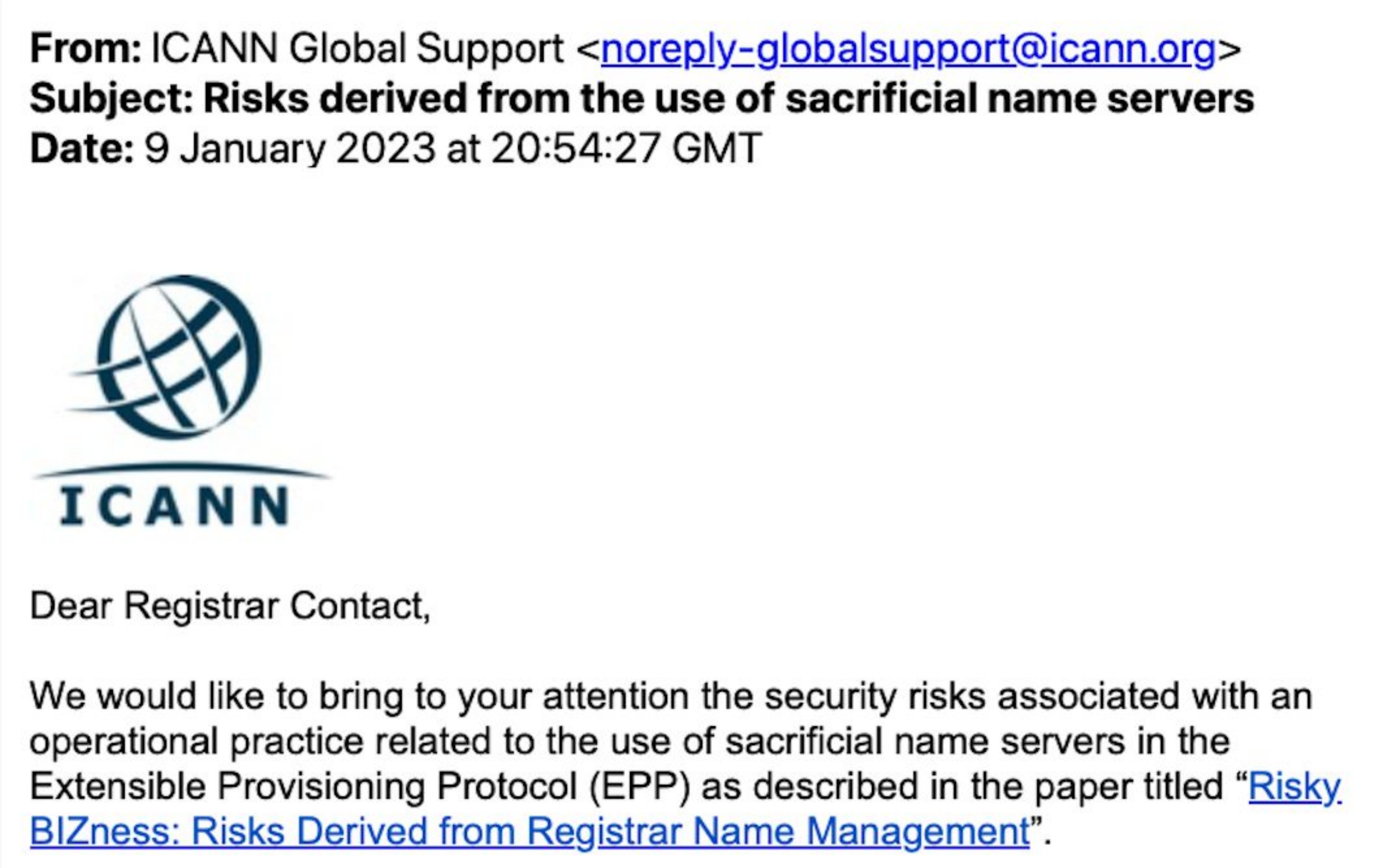
The problem:

- Unintended byproduct of longstanding undocumented registrar practices
- Use of third-party name servers whose domain expires
- EPP + Registry policies prevent removal of such expired domains
    - Goal was to protect other domains that depend on this expired domain

Registrar Workaround

- Rename NS host objects that are subordinate to expired domain
- Rename NS using a new non-existent domain name in another TLD operated by a different registry
    - Allows removal of domain
- Creates new attack surface: someone could register the nonexistent domain name
- Over the last 9 years: > 512K domains have been implicitly exposed to resolution hijacking

Registrar NS Management Work Party



From: ICANN Global Support <noreply-globalsupport@icann.org>
Subject: Risks derived from the use of sacrificial name servers
Date: 9 January 2023 at 20:54:27 GMT

ICANN

Dear Registrar Contact,

We would like to bring to your attention the security risks associated with an operational practice related to the use of sacrificial name servers in the Extensible Provisioning Protocol (EPP) as described in the paper titled "Risky BIZness: Risks Derived from Registrar Name Management".

Registrar NS Management Work Party

The work party:

- Exploring possibilities and requirements for formal description of risk
- Considering approaches to remediate domain resolution hijacking risk
- Investigating options for preventing new exposure

References:

[1] Gautam Akiwate, Mattijs Jonker, Raffaele Sommese, Ian Foster, Geoffrey M. Voelker, Stefan Savage, and KC Claffy. 2020. Unresolved Issues: Prevalence, Persistence, and Perils of Lame Delegations. In Proceedings of the ACM Internet Measurement Conference (IMC '20). Association for Computing Machinery, New York, NY, USA, 281–294. https://www.caida.org/catalog/papers/2020_unresolved_issues/unresolved_issues.pdf

[2]. Gautam Akiwate, Stefan Savage, Geoffrey M. Voelker, KC Claffy, 2020. Risky BIZness: Risks Derived from Registrar Name Management. https://www.caida.org/catalog/papers/2021_risky_bizness/risky_bizness.pdf

Tracking ICANN Top Priorities

- **DNS Abuse**
  - See SAC115: SSAC Report on an Interoperable Approach to Addressing Abuse Handling in the DNS
- **Access to registration data**
  - See SAC118v2: SSAC Comments on Initial Report of the Expedited Policy Development Process (EPDP) on the Temporary Specification for gTLD Registration Data Team – PHASE 2A
  - See SAC101v2: SSAC Advisory Regarding Access to Domain Name Registration Data
  - SSAC sent active representatives to participate in the GNSO's EPDP on the Temp Spec
- **Adding new gTLDs**
  - See SAC114: SSAC Comments on the GNSO New gTLD Subsequent Procedures Draft Final Report
  - See Addendum to SAC114: Additional Context for Recommendation 1, Recommendation 3, Recommendation 7, and Additional References

Topics of Interest/Possible New Work

- Long-term implications of namespace expansion
- Examining datasets available from ICANN for use in the investigation of SSR-related issues that fall within SSAC's remit
- 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:

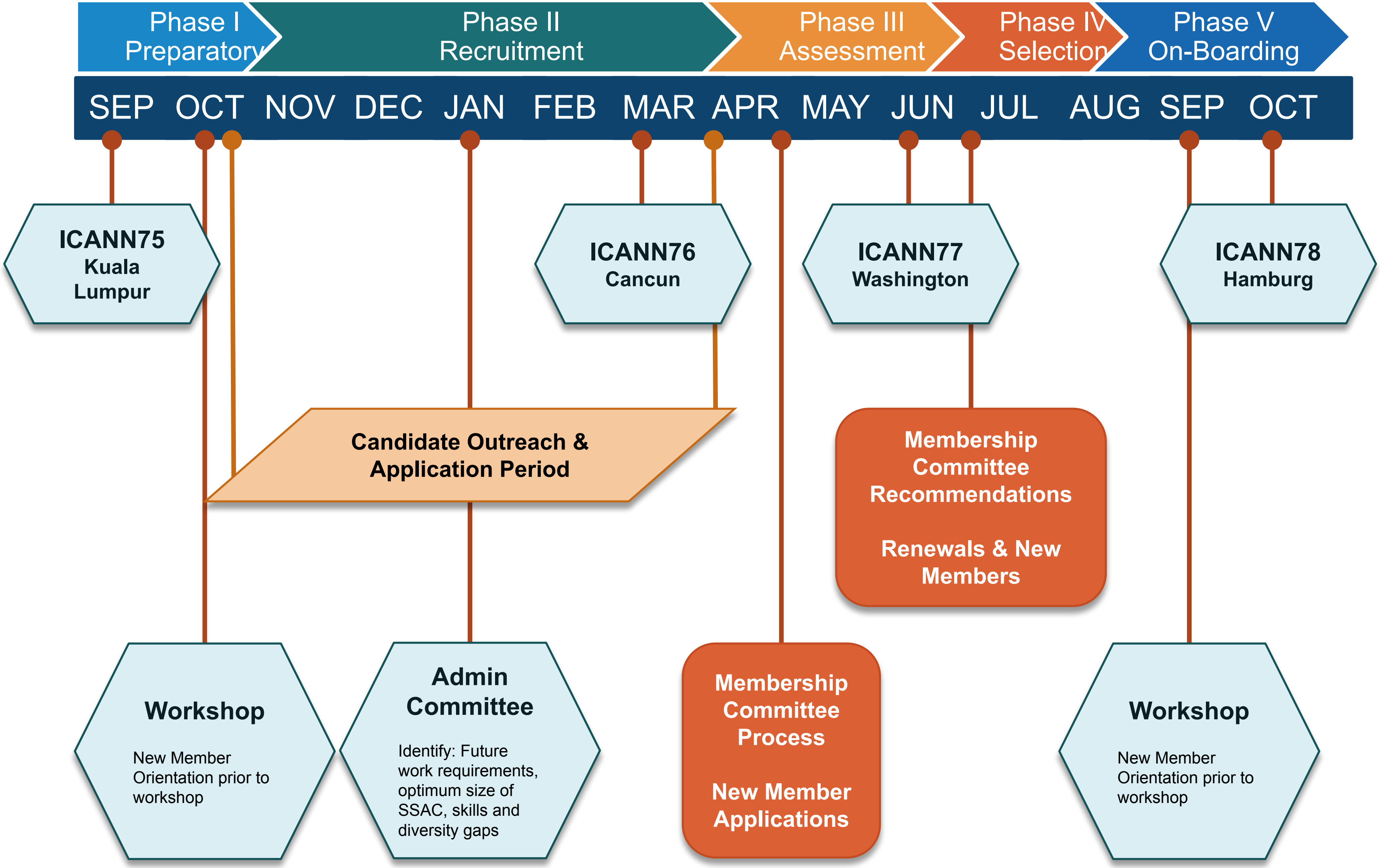
Domain Name System	IP Addressing/Routing
Security	Registration Services
Abuse	Internationalized Domain Names
Root Server System	Information Technology
Non-Technical (e.g., legal, risk management, business skills)	

- 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
    - Large-scale network architecture and design
    - Large-scale Registrar Operations
    - Cloud/hosting experience
    - Browser Development/Testing
    - Mobile Apps Development/Testing
    - Low bandwidth resource constrained Internet connectivity (eg IoT, SCADA)
    - Red Team experience
- The SSAC is interested in increasing membership from Africa, Latin America, and Asia-Pacific
- The SSAC is interested in increasing membership from an academic background

SSAC Membership Outreach – 2023 Timeline



Phase I Preparatory

Phase II Recruitment

Phase III Assessment

Phase IV Selection

Phase V On-Boarding

SEP OCT NOV DEC JAN FEB MAR APR MAY JUN JUL AUG SEP OCT

ICANN75 Kuala Lumpur

ICANN76 Cancun

ICANN77 Washington

ICANN78 Hamburg

Candidate Outreach & Application Period

Membership Committee Recommendations

Renewals & New Members

Workshop

New Member Orientation prior to workshop

Admin Committee

Identify: Future work requirements, optimum size of SSAC, skills and diversity gaps

Membership Committee Process

New Member Applications

Workshop

New Member Orientation prior to workshop

SSAC Contact for Potential New Members

- Individuals who are interested in enquiring about SSAC membership should:
  - Review information on the SSAC Public Website: https://www.icann.org/groups/ssac,
  - Contact any member of SSAC Support Staff, or
  - Send an email to ssac-staff@icann.org

2023 Notable Events

- SSAC will commence the process to elect a new Chair and Vice Chair in May 2023

Thank you