ICANN 77
POLICY FORUM
WASHINGTON, D.C.
12-15 June 2023

SSAC Activities Update

Rod Rasmussen, SSAC Chair
ICANN77 | June 2023

Agenda

- SSAC Overview
- SSAC Chair and Vice Chair Elections for 2023
- 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

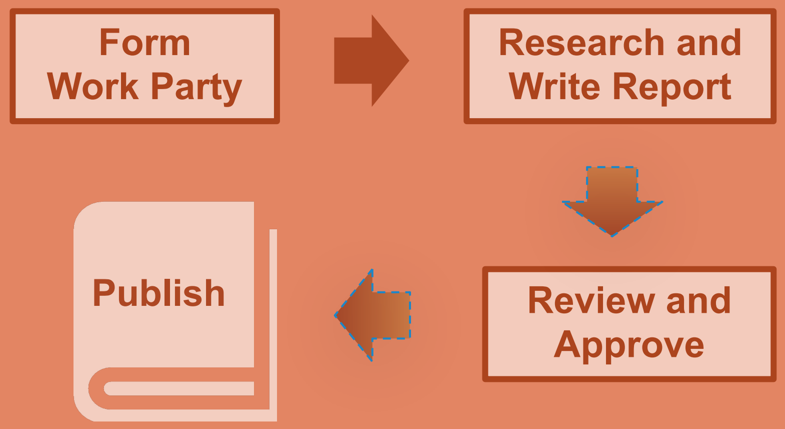
121 Publications since 2002

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

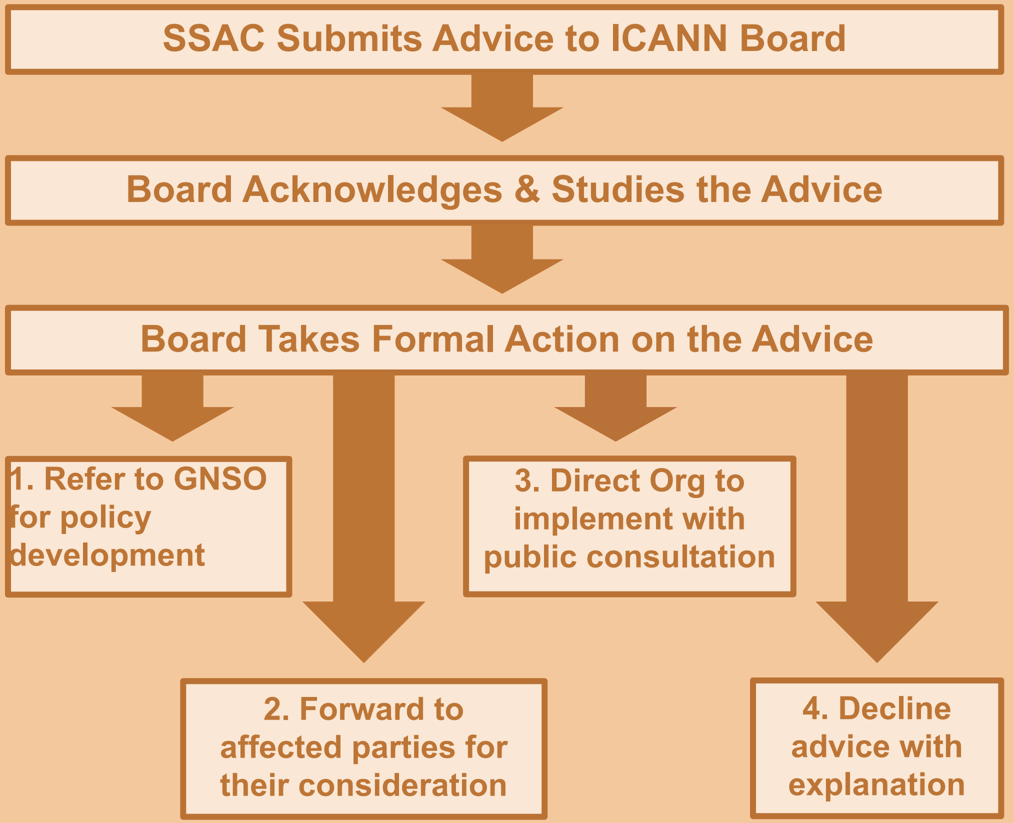
Research and Write Report

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

SSAC Chair and Vice Chair Elections for 2023

- SSAC is running consecutive Chair and Vice Chair elections this cycle instead of concurrent elections
- SSAC Chair Election proceedings commenced on 10 May 2023
  - SSAC has selected Ram Mohan as the next SSAC Chair
- SSAC Vice Chair Election proceedings will commence on 11 July 2023
- SSAC expects to select the Vice Chair by 7 August 2023
- Chair and Vice Chair terms officially begin on 1 January 2024 and last through 31 December 2026

Name Collision Analysis Project

Matt Thomas and Suzanne Woolf

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 - Key Findings So Far

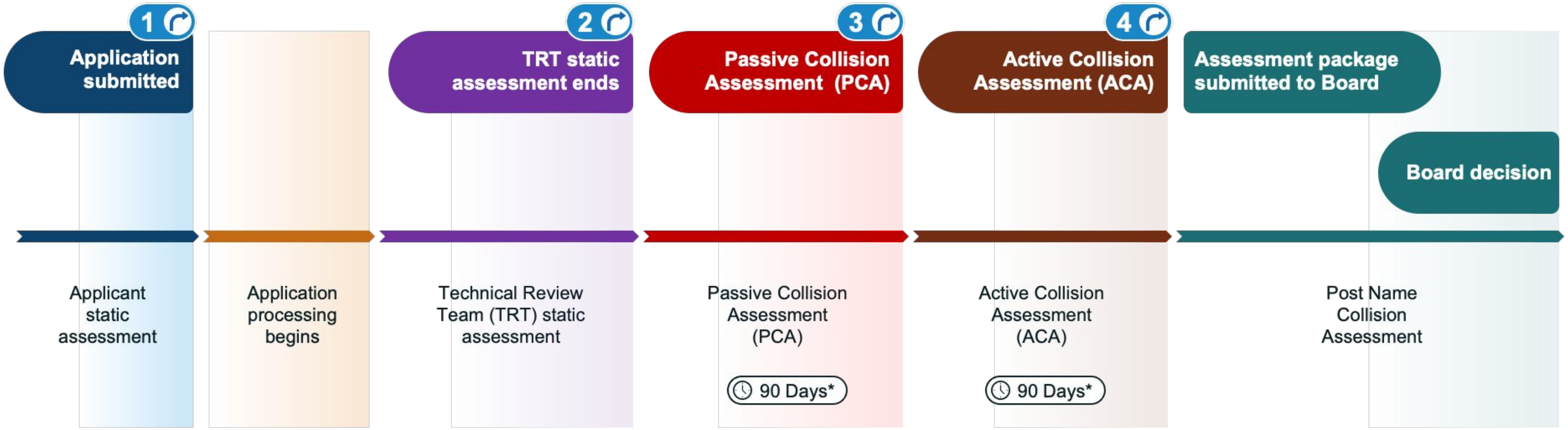
- Query Volume
- Query Origin Diversity
  - IP address distribution
  - ASN distribution
- Query TYPE Diversity
- Label Diversity
- Other characteristics
  - Open-Source Intelligence (OSINT)

- **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/1PDIX6sMldP4vLn1LLuefxsup78mLM0iDb8ybWhlw2T4/edit

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

Updates on SSAC Work Parties

DNSSEC DS Automation

Current Work Parties

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

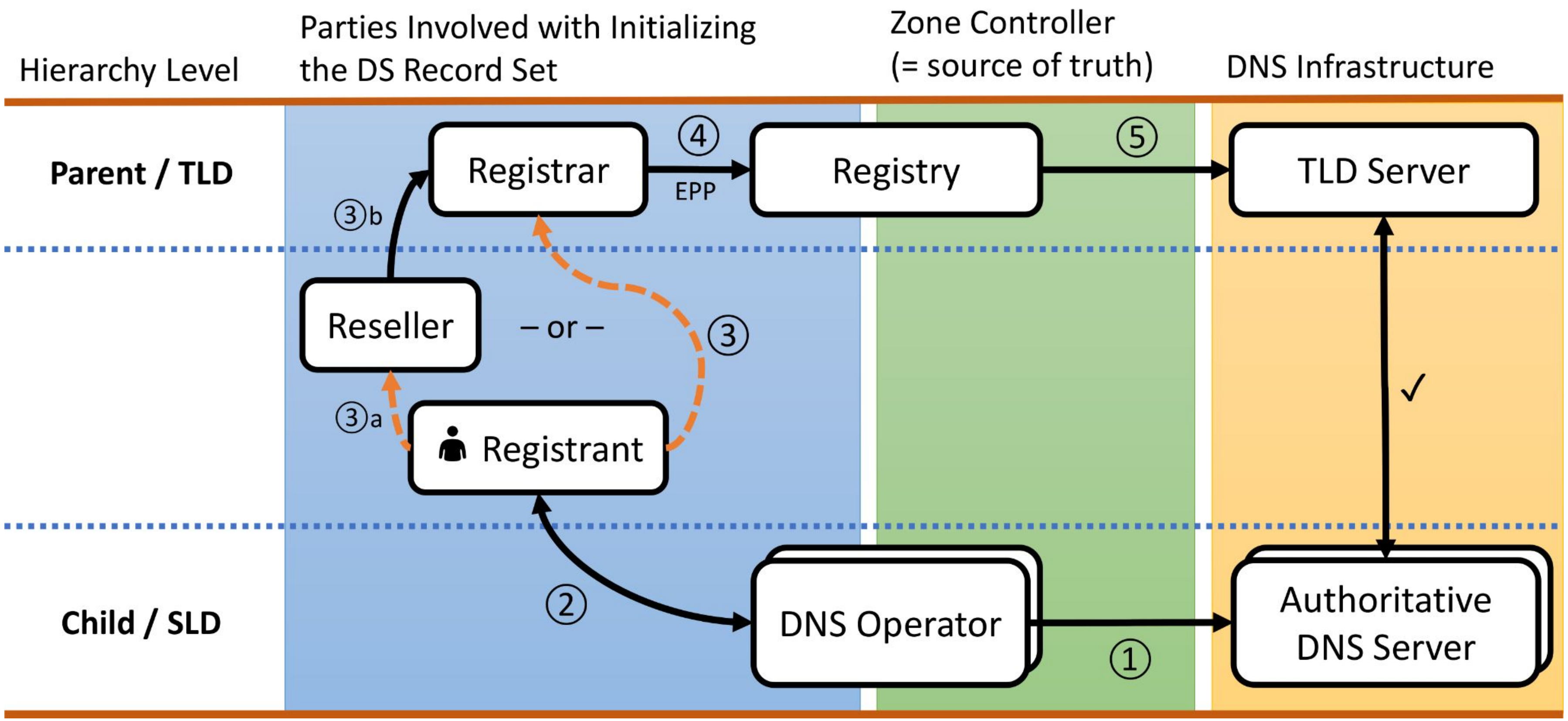
Updates on SSAC Work Parties

DNSSEC DS Automation

DS Automation - Considerations

- Proper DNSSEC operation requires periodic changes to the keys used to sign a zone.
- Whenever the KSK is changed, the corresponding DS record in the parent zone needs to be updated.
- If a registrant’s DNS service is provided by a 3rd party DNS provider unrelated to the registrar, there is no uniform and widely implemented method for causing a new DS record to be put into the parent registry.
- All registrars that support DNSSEC provide a web interface that supports manual insertion of a new DS record.
- Manual update of DS records is onerous and error-prone. It is perceived as **frustrating** and **difficult**, this has become one of the choke points for DNSSEC adoption.
- There are multiple ways to automate DS updates - the differentiation is whether DS updates are conveyed directly to the registry or to the registrar. Both methods are already in use.

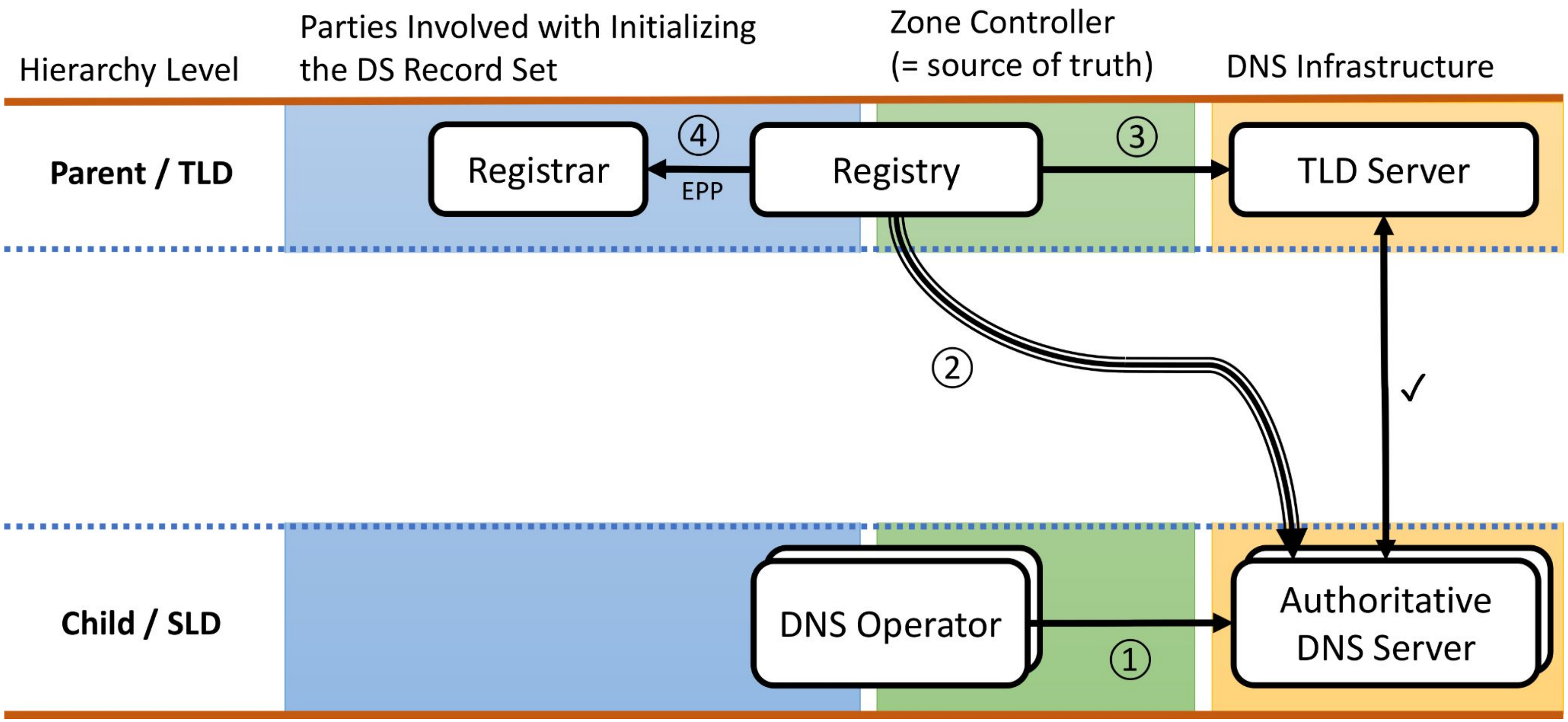
DS Automation - Current Process



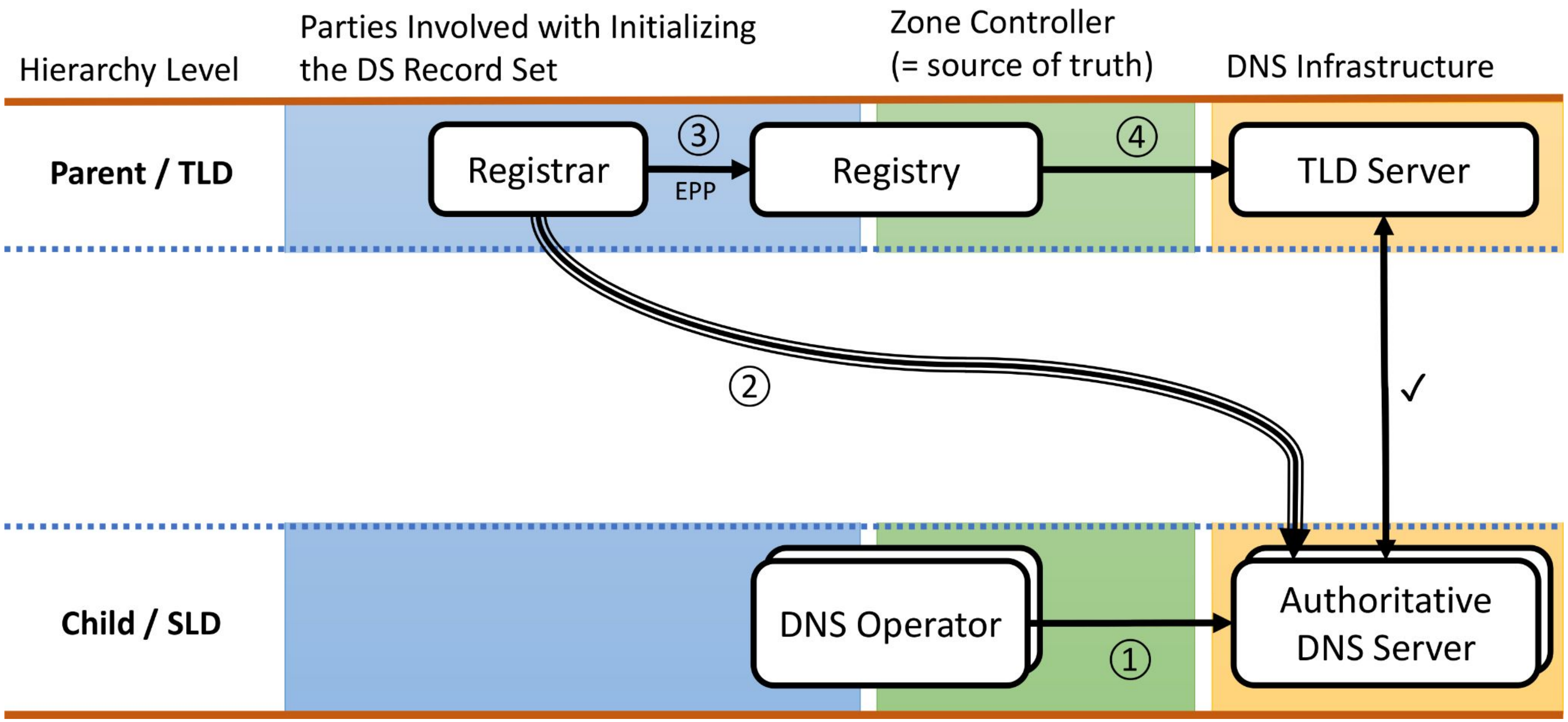
DS Automation - Considerations

- Current implementations are based on scanning. Scanning has two potential defects. Sending a NOTIFY when the child’s key is changed alleviates both defects.
  - Scaling: It may pose a load on the system. (Though based on the data we have so far, scaling does not appear to be a problem.)
  - Delay: Scanning takes time to detect changes.
- Implementation of NOTIFY requires a further technical specification as to where to send the NOTIFY and software development to accept and act on the NOTIFY.
- **Concern:** There is a potential for confusion if both the registry and the registrar automate DS updates. This can be eliminated if the registry and registrar agree that only one of them will automate DS updates.

DS Automation - Model 1



DS Automation - Model 2



DS Automation - Preliminary Positions

- Automation of DS updates should be required functionality. All registries and registrars should provide this.
- ICANN Org should take a proactive posture to hasten DS automation. ICANN Org should advocate DS Automation across all domains, gTLDs, ccTLDs and RIRs.
- The ideal arrangement is to have DS updates conveyed to the registrar. This conforms to the basic Registry-Registrar-Registrant (RRR) model.
- Conveyance directly to the registry is an acceptable implementation and should not be discouraged. Further, registries can automate DS updates and then delegate the function to their registrars. The delegation can be incremental with those registrars with the necessary capability.
- All DNS operators, including those which are part of registrars, should have the capability of executing NOTIFY commands when either the KSK or ZSK changes. This may seem unnecessary for ZSK changes or for KSK changes made by registrar-operated DNS services, but it will be necessary for future DNSSEC coordination.

Updates on SSAC Work Parties

Registar NS Management

Registar NS Management - Problem Statement

- **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

Registar NS Management - Scope

- Building on the risks identified in the paper ***Risky BIZness: Risks Derived from Registrar Name Management***
- Exploring the risks that emerge from the expiration of domains that other domains rely on for authoritative name service
- The SSAC is also investigating options for detection, remediation for domains that are currently exposed, and operational practices that will prevent new exposures
- For each options to mitigate current exposures and prevent new exposures the SSAC is reviewing
  - ***Benefits*** of each option to registrars, registries, and registrants
  - ***Burdens*** to registrars, registries, and registrants
  - ***Residual risk*** if the option is implemented

Updates on SSAC Work Parties

Evolution of DNS Resolution

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

- 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.
- 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.

Tracking ICANN Top Priorities

- **DNS Abuse**
  - See SAC115: SSAC Report on an Interoperable Approach to Addressing Abuse Handling in the DNS
  - SSAC is reviewing the recently published contract amendments
- **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
- DNSSEC Assessment and examining the potential for DNSSEC as a universal trust anchor

SSAC Skills and Potential New Member Outreach

Julie Hammer

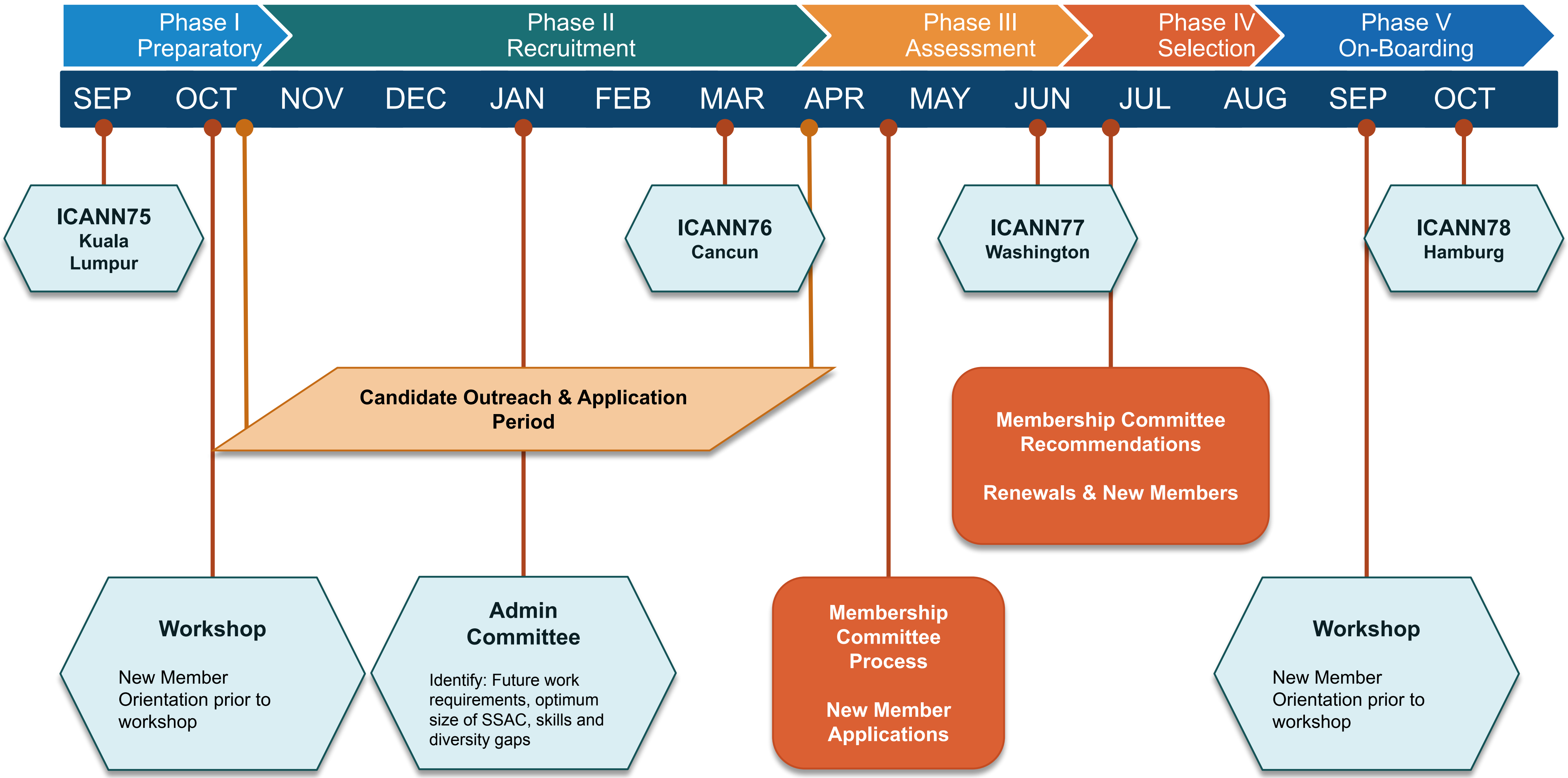
SSAC Member Skills

- 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
  - 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