ICANN 76
COMMUNITY FORUM
CANCÚN
11-16 March 2023

Joint Meeting: SSAC & ALAC
12 March 2023

Agenda

- **ALAC Topics:**
  - BC/IPC/ALAC To the ICANN Board: Improvements to 2013 Registrar Accreditation Agreement (RAA) and Current Registry Agreement (RA)
  - ALAC to the ICANN Board: Comments and Concerns on the SubPro Operational Design Assessment (ODA)
  - DNS Abuse
- **SSAC Topics:**
  - NCAP (Matt and Suzanne) 5-minutes
  - Evolution of DNS Resolution (Barry and Russ H.) 10-minutes
  - DNSSEC DS Automation (Peter and Steve)10-minutes
  - Registrar NS Management (Rod) 5-minutes
  - SSAC New Member Outreach (Julie) 5-minutes

ALAC Questions

ALAC Topic

- BC/IPC/ALAC To the ICANN Board: Improvements to 2013 Registrar Accreditation Agreement (RAA) and Current Registry Agreement (RA)

ALAC Topic

- ALAC to the ICANN Board: Comments and Concerns on the SubPro Operational Design Assessment (ODA)

ALAC Topic - DNS Abuse

- SSAC perspective on long term plan:
  - A strategic plan to mitigate DNS abuse can drive specific work and/or policy development over the course of time. A strategic plan should accomplish at least these tasks:
    - Explore all aspects of mitigating DNS Abuse including proactive prevention, detection, information sharing, effective approaches, community standards, shared expectations, and overall goals.
    - Create a consistent, consensus baseline for market participants and a regime to measure results to ensure such a baseline is met and maintained over the long term.
    - Develop and communicate a set of processes and expectations for the anti-abuse community to utilize in order to effectively collaborate to mitigate DNS Abuse.
    - Create a work plan with a timeline and participants from the community to meet these goals.
  - Concerns regarding expansion of new gTLDs

ALAC Topic - DNS Abuse

- Combined concerns about understanding concentrations of DNS abuse in the 2012 round of the new gTLD program
  - Alignment of existing recommendations from SSAC, ALAC, GAC, CCT Review
  - Create a combined statement that we can provide that is constructive to the overall process

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)

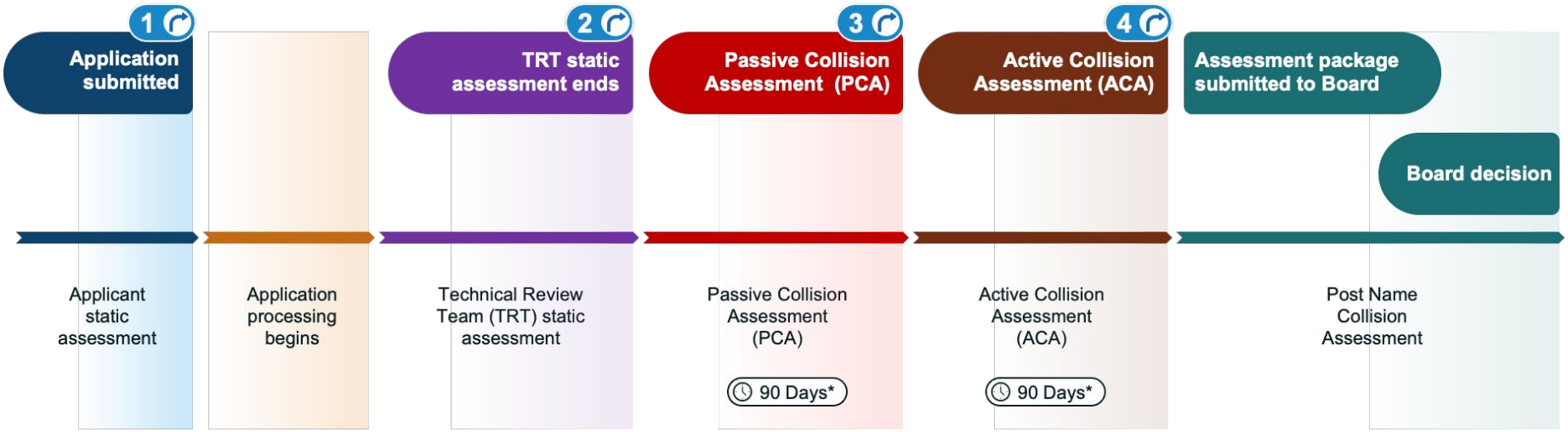
- **Impact (or Harm) is determined by evaluating both Volume and Diversity across all CDMs**

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



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?

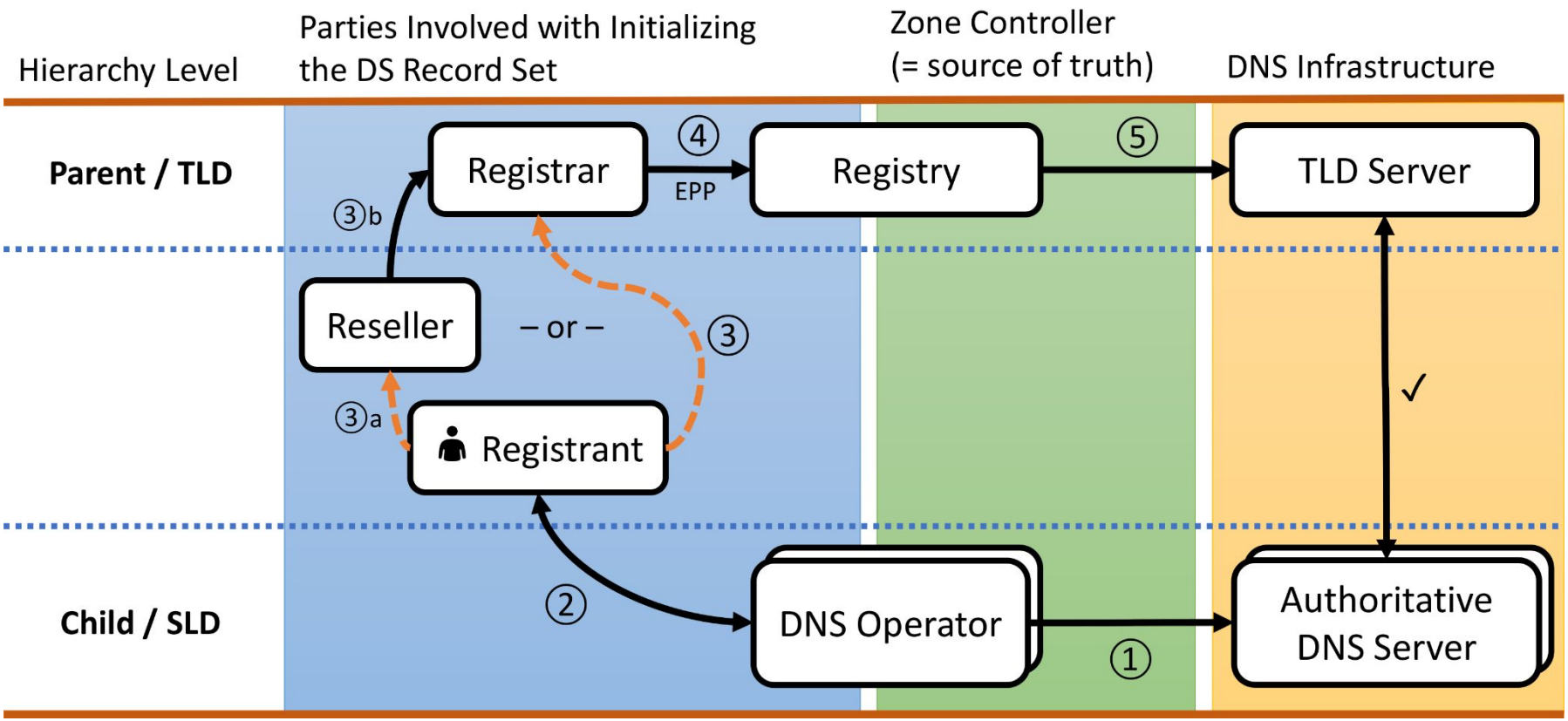
- Four responsibilities
  - Operate Passive Collision Assessment environment
  - Operate Active Collision Assessment environment
  - Log processing and analysis preparation for TRT
  - Emergency response

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

DS Automation - Current Process



Considerations From a Registrant Perspective

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.**

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

SSAC DS Automation Work Party

- **Goal:** Develop recommendations for automated management of DS records
- **Deliverable:** An advisory that explains the issues, surveys the possible solutions, and provides recommendations to registries, registrars, and DNS service providers to facilitate the automatic initialization and updating of DS records
- **Rough timeline:** By ICANN 77

SSAC Registrar NS Management Work

- Certain operational practices between domain registrars and registries are designed to work around EPP requirements that prevent the deletion of host name objects that are referenced by other domain objects.
- Recent work has shown that due to the workaround practices, over the last nine years over 512K domains have been implicitly exposed to hijacking, affecting names in most popular TLDs (including .com and .net) as well as legacy TLDs with tight registration control (such as .edu and .gov).
- Multiple parties have actively exploited this weakness, assuming control over 163K domains without having any ownership interest in those names.
- The goal of SSAC work party is to identify reasonable operational practices for registrars to adopt to prevent new hijacking risks from arising as well as addressing domains currently at risk.

SSAC Skills and Potential New Member Outreach

Julie Hammer

SSAC Member Skills

- The skills of SSAC members span the following categories:

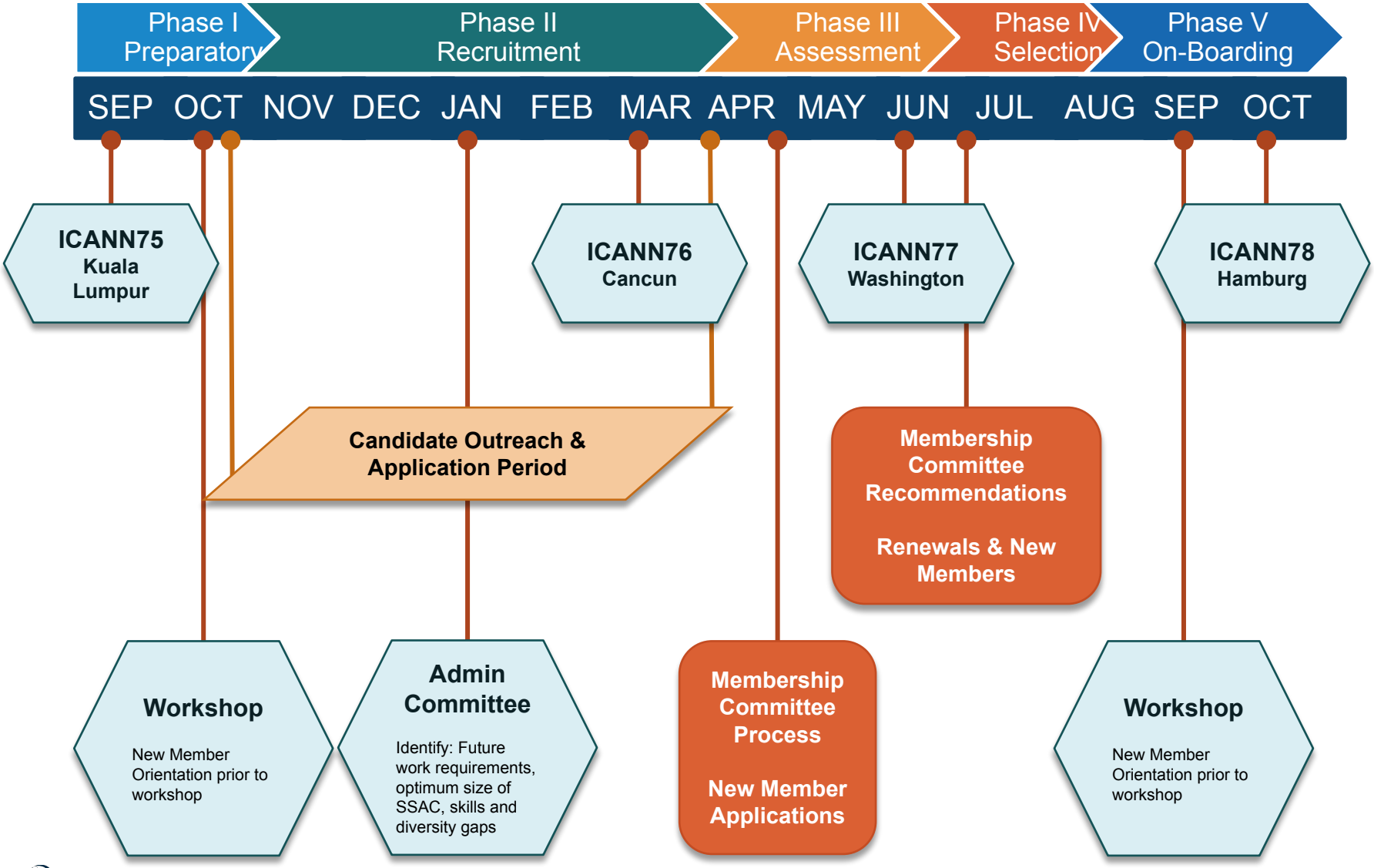
Domain Name System	IP Addressing/Routing
Security	Registration Services
Abuse	Internationalized Domain Names
Root Server System	Information Technology
Non-Technical (e.g., legal, risk management, business skills)	

- 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



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

Thank you