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

Joint Session: ALAC/SSAC

Rod Rasmussen, SSAC Chair
ICANN77 | June 2023

Agenda

- **Welcome and Opening Comments - Jonathan Zuck, ALAC Chair and Rod Rasmussen, SSAC Chair (5 mins)**
- **SSAC Topics (55 mins)**
  - Update on the DS Automation Work Party
  - Alignment on the next Round
  - Collision Work
  - Registar NS Management Work Party Update
  - Review of Inputs to the Transfer Policy Review PDP
- **ALAC Topics (10 mins)**
  - Alignment on .Zip
- **Closing Comments and Next Steps - Jonathan Zuck, ALAC Chair and Rod Rasmussen, SSAC Chair (5 mins)**

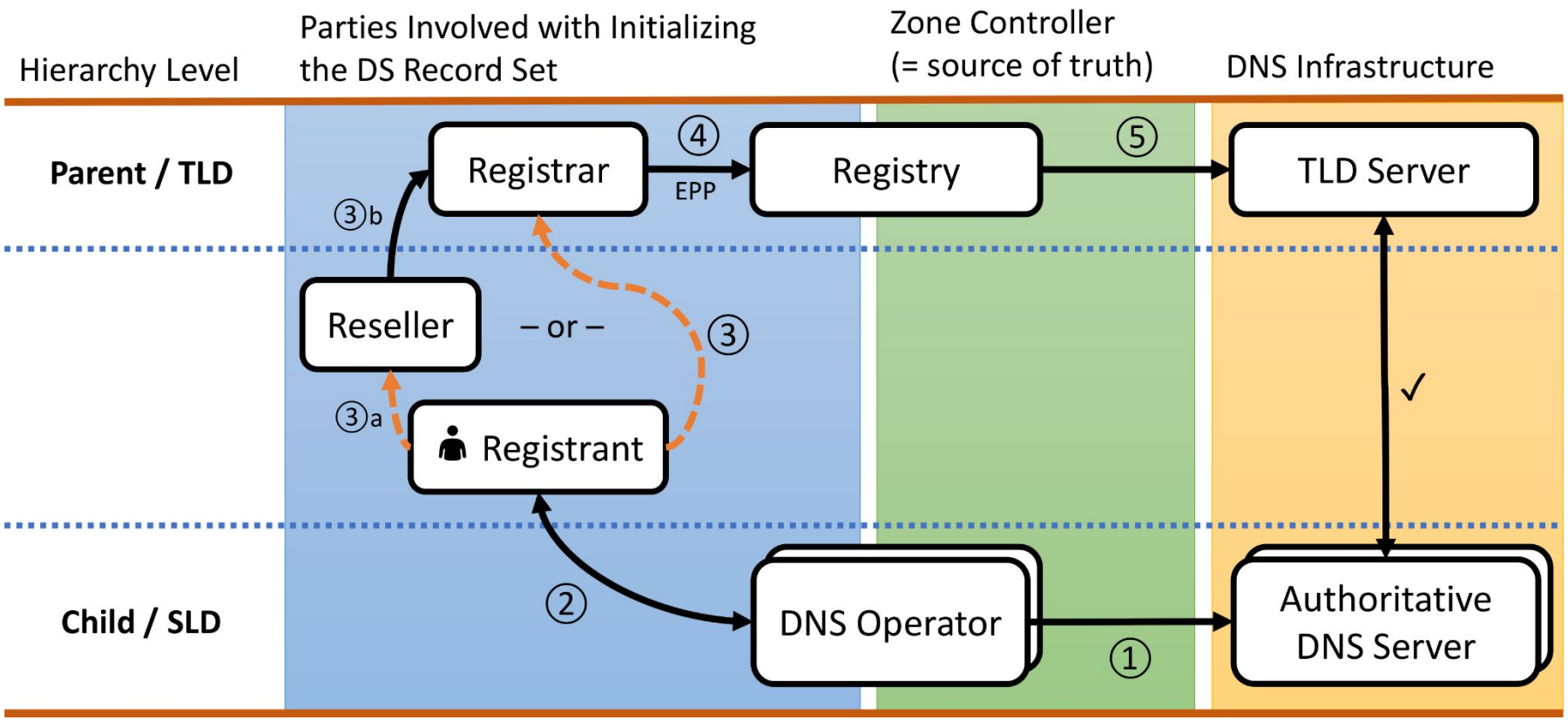
Updates on SSAC Work Parties

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.

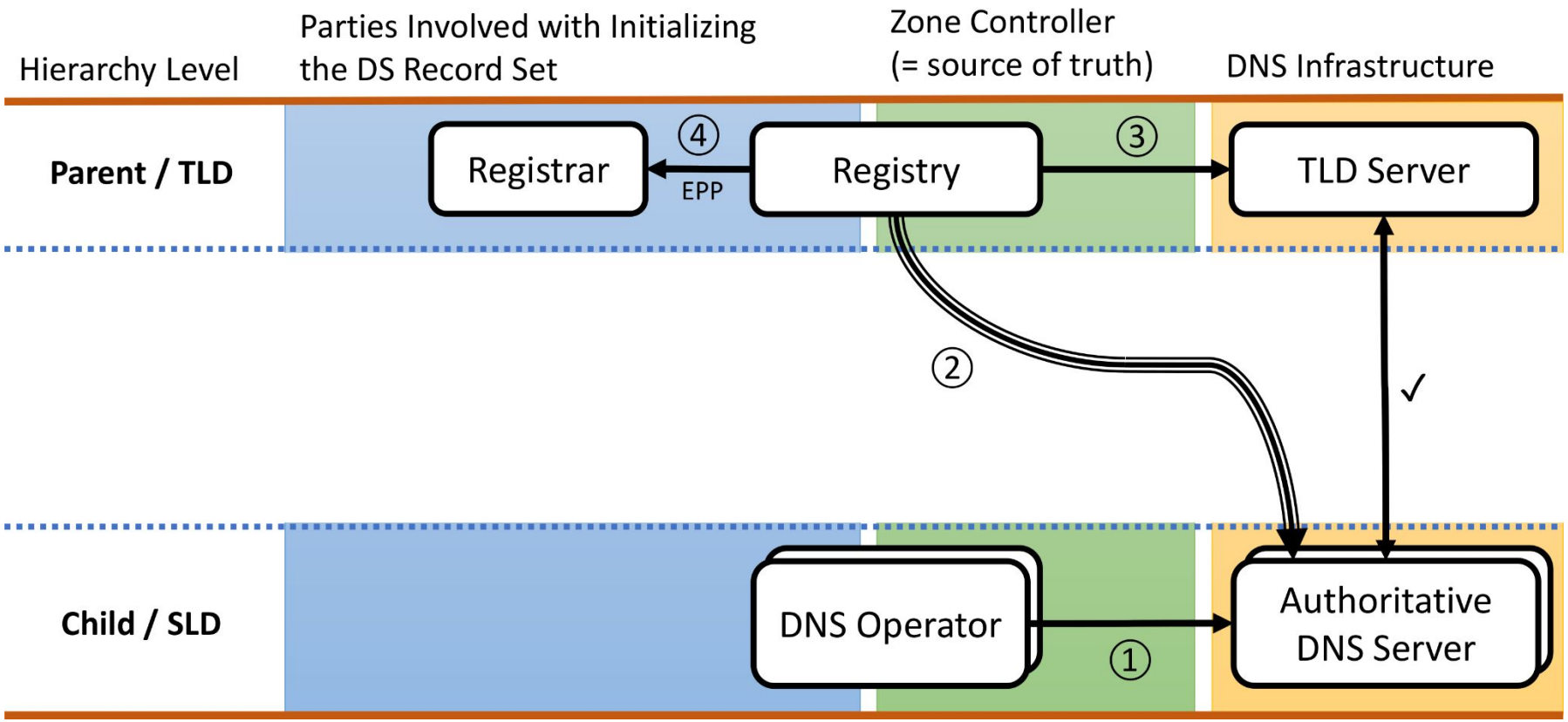
DS Automation - Current Process



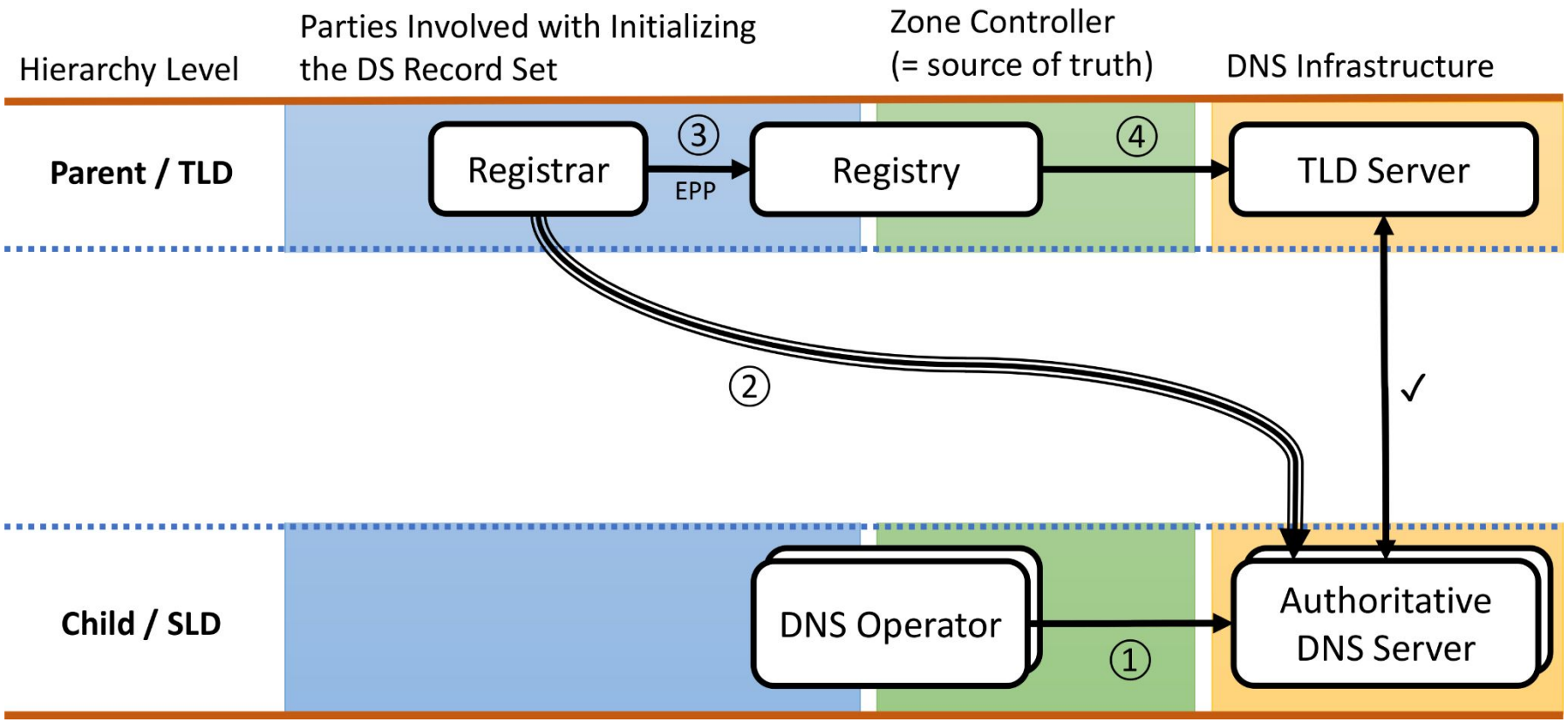
DS Automation - Considerations

- 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.

Alignment on the Next Round of the New gTLD Program

DNSSEC DS Automation

Alignment on New gTLD Program Next Round Implementation

- Are there any outstanding safety or security issues that need to be address in the implementation of the New gTLD Program next round?

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

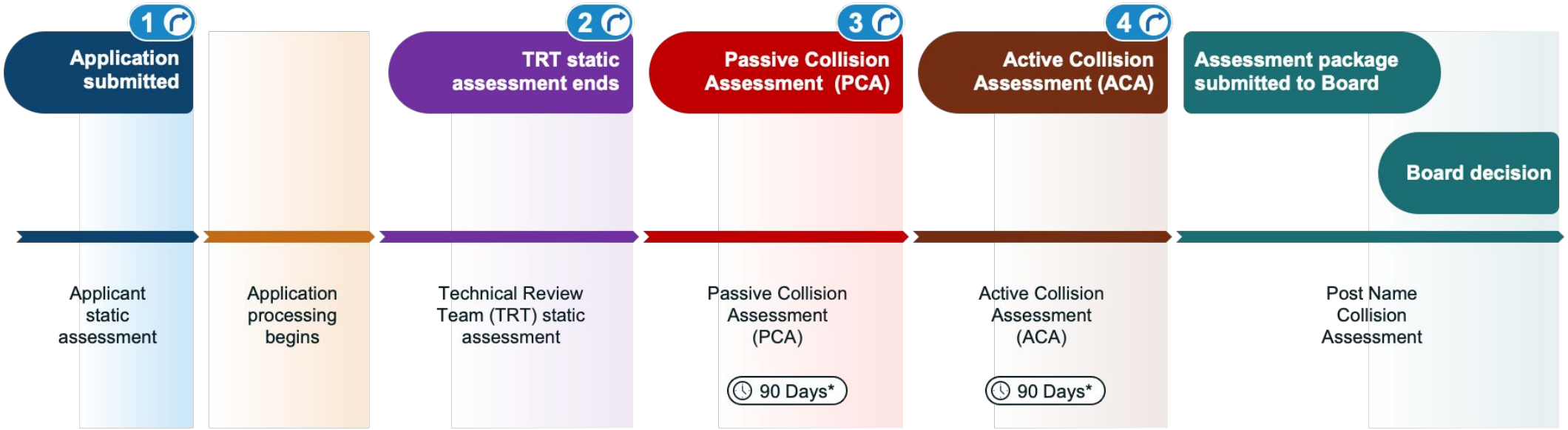
- Query Volume
- Query Origin Diversity
  - IP address distribution
  - ASN distribution
- Query TYPE Diversity
- Label Diversity
- Other characteristics
  - Open-Source Intelligence (OSINT)

- **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



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/1PDIX6sMIdP4vLn1LLuefxsup78mLM0iDb8ybWhIw2T4/edit

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

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

Review of Inputs to the Transfer Policy Review PDP

Review of Inputs to the Transfer Policy Review PDP

- SAC119: Feedback to the GNSO Transfer Policy Review PDP WG (5 August 2021)
  - SSAC believes that it is important for registrants to experience a secure, stable, and smooth transition when transferring registrations between registrars.
  - There are two specific security risks the SSAC highlighted:
    - A registrant's domain name is at risk of experiencing a discontinuity of DNS resolution, and when DNSSEC is in use, a discontinuity of validation, during a registration transfer if the transfer of DNS services is not considered during the process.
    - A registrant's domain name is at increased risk of being hijacked if the authInfo code is not managed according to best practice security principles.
-

Review of Inputs to the Transfer Policy Review PDP

- SSAC2022-06: SSAC Input to the GNSO Transfer Policy Review PDP WG on DNSSEC (19 July 2022)
  - SSAC reiterated one of the risks documented in SAC119: a registrant's domain name is at risk of experiencing a discontinuity of DNS resolution and DNSSEC validation, if the transfer of DNS services is not considered during the process.

- SSAC Response to GNSO Transfer Policy Review Working Group on Group 2 Topics (27 April 2023)

ALAC Topic: Alignment on .ZIP