ICANN 79 COMMUNITY FORUM

Joint Session
SSAC and RSSAC

Agenda

- Opening Remarks, Agenda Bashing
- Overview of Active RSSAC Caucus Work Parties (RSSAC lead)
- Presentation of the RSS for the Public Interest (Jeff Osborn)
- NCAP Study 2 Recommendations: References to the Root Zone (Matt Thomas, Suzanne Woolf)
- Open discussions / AoB (SSAC and RSSAC Members)

Format for Open Session

- **Participation:** Discussion and presentation are reserved for committee members.
- **Questions:** Time permitting, Chairs may open the floor for Q&A at the end of the agenda
- **For direct engagement with RSSAC members check out**
  - **Session:** How it Works Session #2: Root Server Operations
    - **Agenda:** Introduction ICANN participants to the Root Server System (RSS) and its operation
    - **When:** Sunday, Block 3, Room 209 ABC (ccNSO)
- **For direct engagement with SSAC members check out**
  - **Session:** SSAC Public Meeting
    - **Agenda:** SSAC will provide updates to the ICANN community on SSAC's View on Name Collision Analysis Project, briefing on recent SSAC publications, and SSAC's current priorities
    - **When:** Wednesday, Block 2, Room 208 BC
  - **Session:** SSAC Open Forum, listed as "SSAC Work Session (8 of 8)"
    - **Agenda:** Informal, drop-in-style session is your opportunity to connect directly with SSAC members and discuss various topics
    - **When:** Thursday, Block 1, Room 103 B

Introductions

All

Overview of recent RSSAC Publications and Active RSSAC Caucus Work Parties

RSSAC

Security Incident and Reporting Work Party (Ken)

- RSSAC058 A.1.1.1 states
  - The RSS GS must include provision for cyber incident oversight and disclosure obligations, and codify security threat and vulnerability information sharing amongst RSOs and the RSS GS Body.
- RSOs have been doing this informally
- The RSSAC Caucus Security Incident Reporting Work Party is now in progress
  - It will provide more formal advice to the Root Server System Governance Structure (RSS GS) on this.

Confidentiality and Log Anonymization (Ken)

4.4 Confidentiality

In many parts of the world IP addresses are considered as personally identifiable information (PII), so packet captures and log files which contain IP addresses and associate them with query names should be considered confidential. There are also existing and newly defined protocols (e.g., DoT, DOH, QUIC) which protect query names in transport.

- If an RSO supports encrypted transports, compromise of keying material should be reported.
- Unauthorized exposure of non-anonymized DNS query logs or packet captures
- Unauthorized exposure of confidential information necessary for the operational security of an RSO should be reported. For example, loss of SSH private keys necessary for management of instances.

https://docs.google.com/document/d/1NvSw7PoLGYhXPuMEjiBgqjCtp_khTGGEh0DaHkNJdds/

Overview of the RSS for a Public Interest Audience

Jeff Osborn

NCAP Study 2 Recommendations

Matt Thomas and Suzanne Woolf

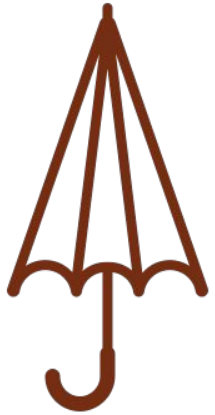
Name Collision Assessment Framework

NCAP Study 2 proposes a comprehensive Name Collision Risk Assessment Framework to safeguard the DNS from potential disruptions caused by name collisions.

Key Features of the Risk Assessment Framework:

- **Integrated Risk Assessment:** Embeds name collision assessment into the broader review process for new gTLD string applications.
- **Technical Review Team (TRT):** Introduces a dedicated team to evaluate proposed new gTLD strings based on empirical analysis.
- **Enhanced Data Collection:** Encourages the collection of additional quantitative and qualitative data from publicly available datasets for a more comprehensive risk assessment.
- **Multiple Assessment Methods:** Offers four methods for collecting and analyzing data to assess risk.

Goals of Proposed Name Collision Risk Assessment Framework



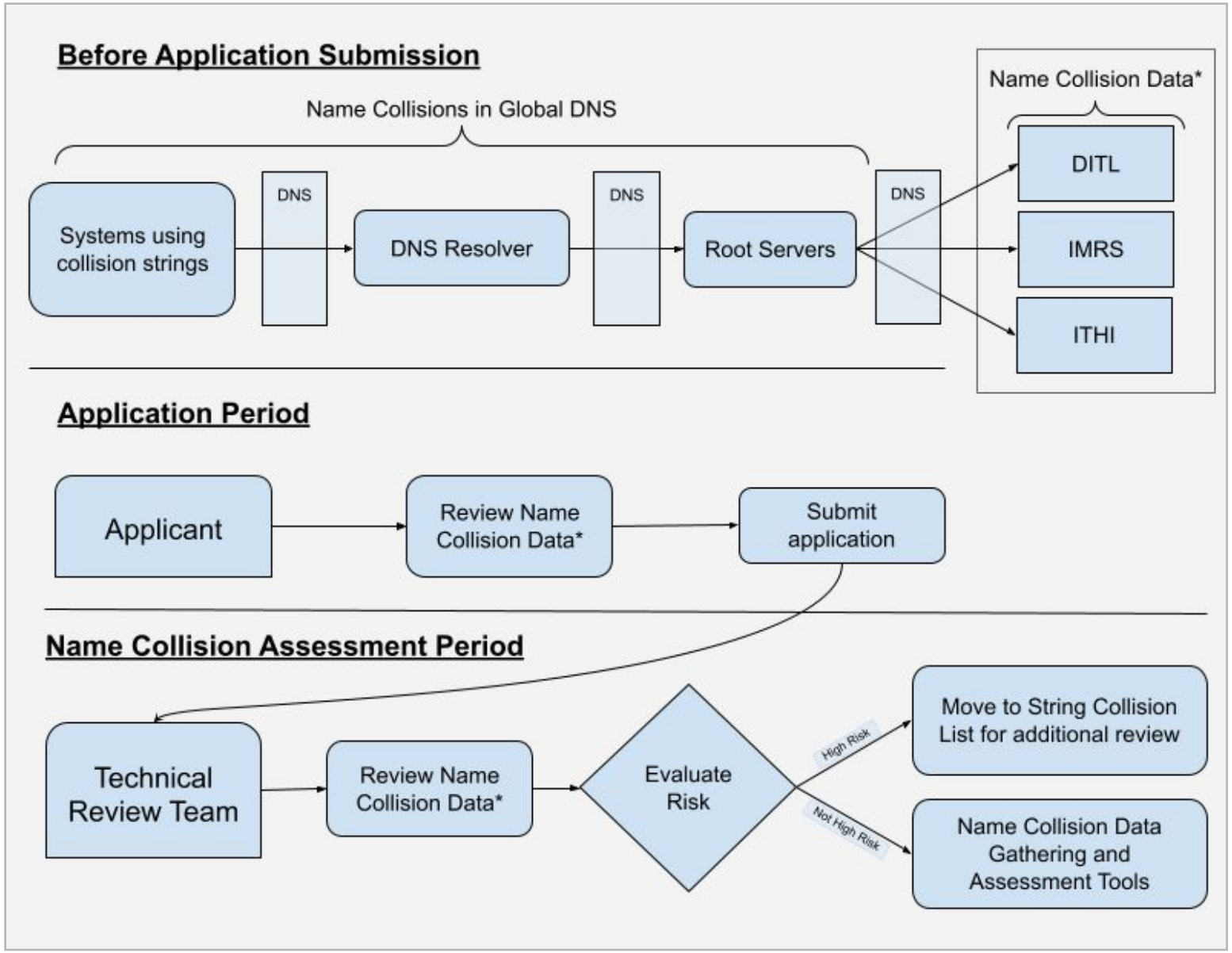
Goal 1: Ensure that name collisions can be assessed

- Root zone delegation is required for empirical analysis of potential name collisions
- Requires ability to define, collect, and analyze relevant measurements (see Study 2 Report)

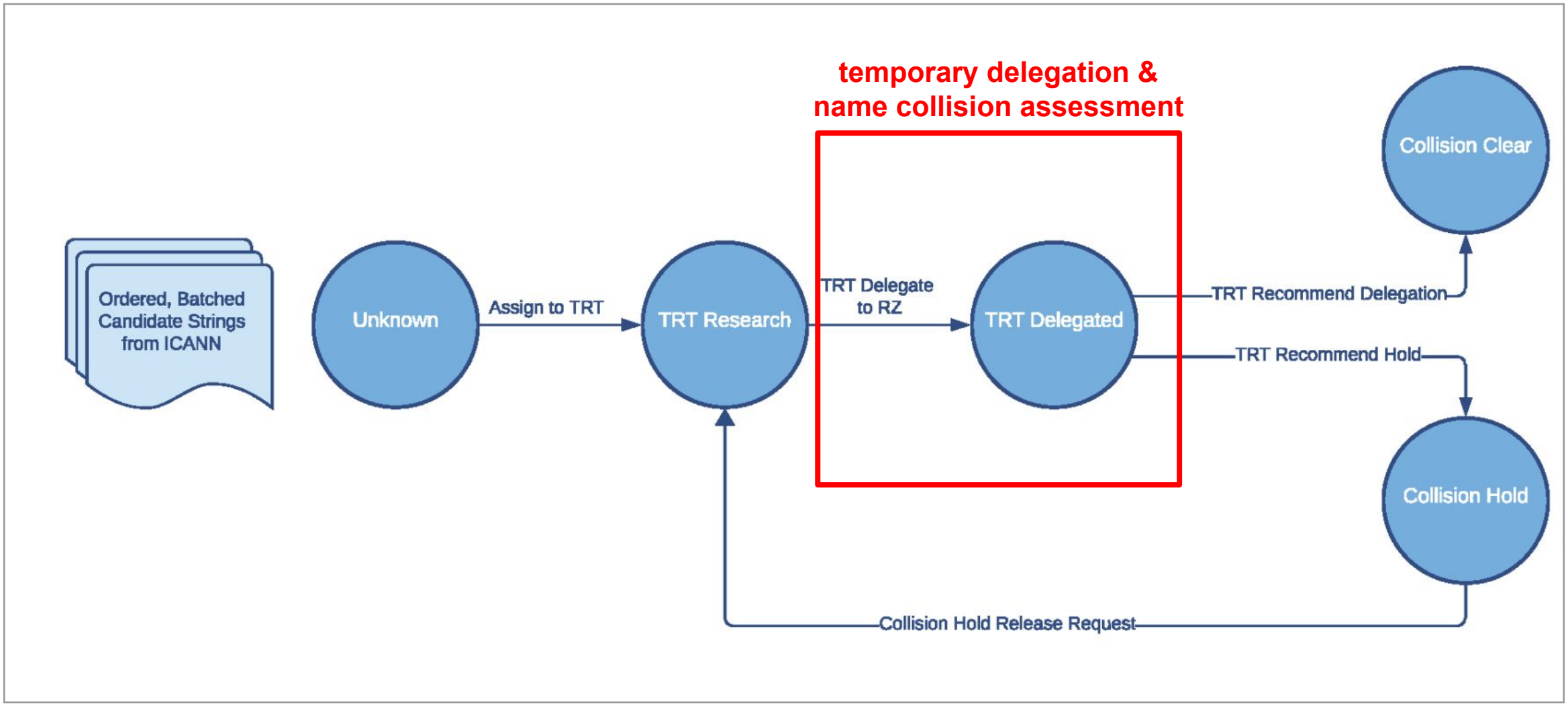
Goal 2: Provide a process for ICANN to evaluate mitigation and remediation plans for identified name collisions

- While known causes may inform mitigation and remediation plans, further investigation may be required for specific labels
- Ensures that a mitigation or remediation plan (or both) can be developed and assessed

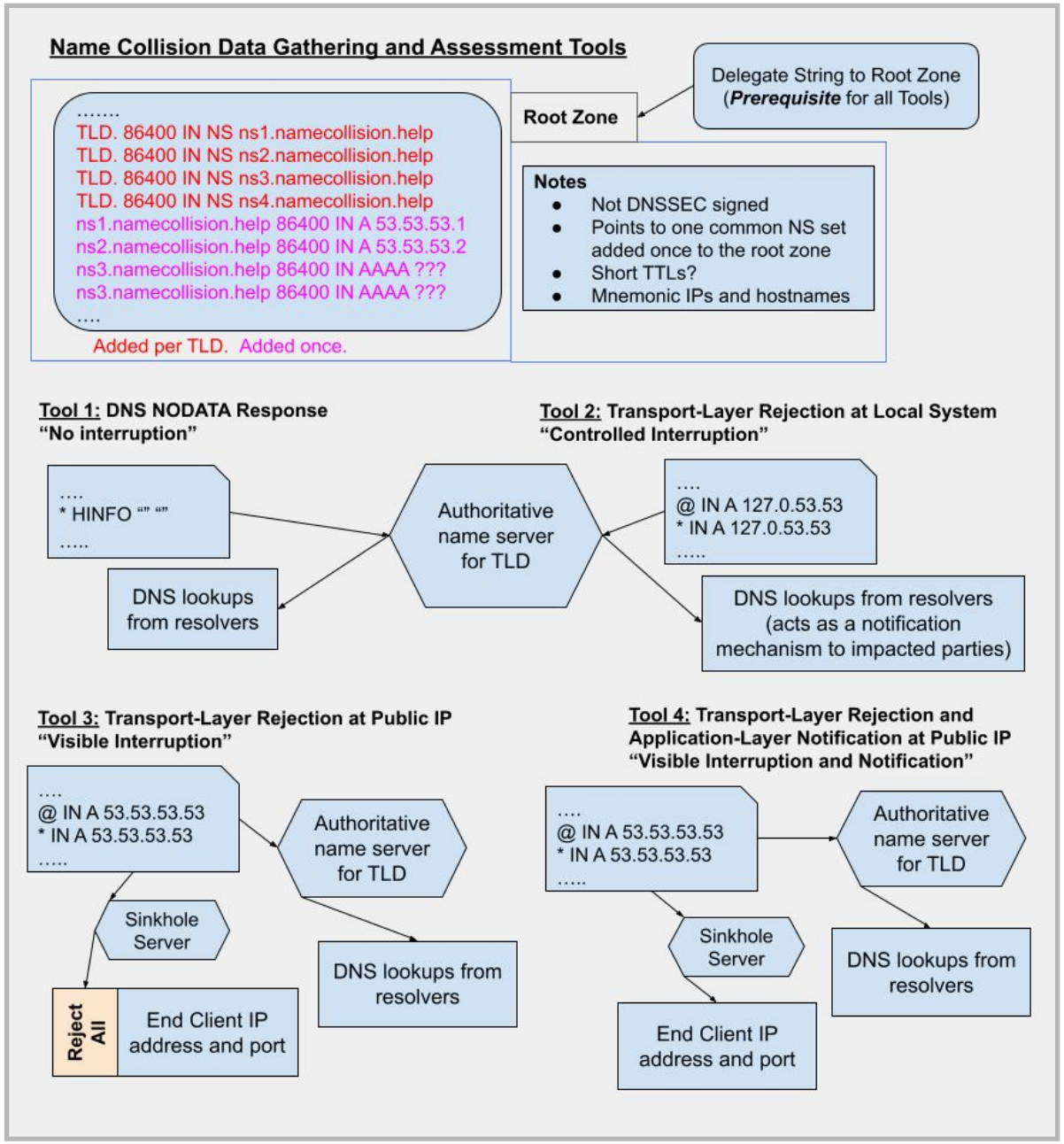
Initial workflow in the proposed Name Collision Risk Assessment Framework



Representation of Technical Review Team workflow for assessing strings



Data collection tools in the proposed Name Collision Risk Assessment Framework



NCAP Study 2 Recommendations: References to the Root Zone

Emergency Change Process for the Removal of Temporary Delegation:

- ➔ NCAP Recommendation: Establish a process for removing a temporary delegation where the assessment process results in unacceptable risk to internet services.
- ➔ RSSAC might need to be consulted when defining the emergency change process

NCAP Study 2 Recommendations: References to the RSS

Updated Name Collision Assessment Methods:

- ➔ NCAP Recommendation: Develop and implement improved methods for assessing potential name collisions, incorporating data beyond root servers for a more comprehensive evaluation.
- ➔ Some RSO involvement may be needed provide data from root servers to support improved name collision assessments

Open Discussion and Any Other Business

All