ICANN 79 COMMUNITY FORUM

Insights from the SSAC:

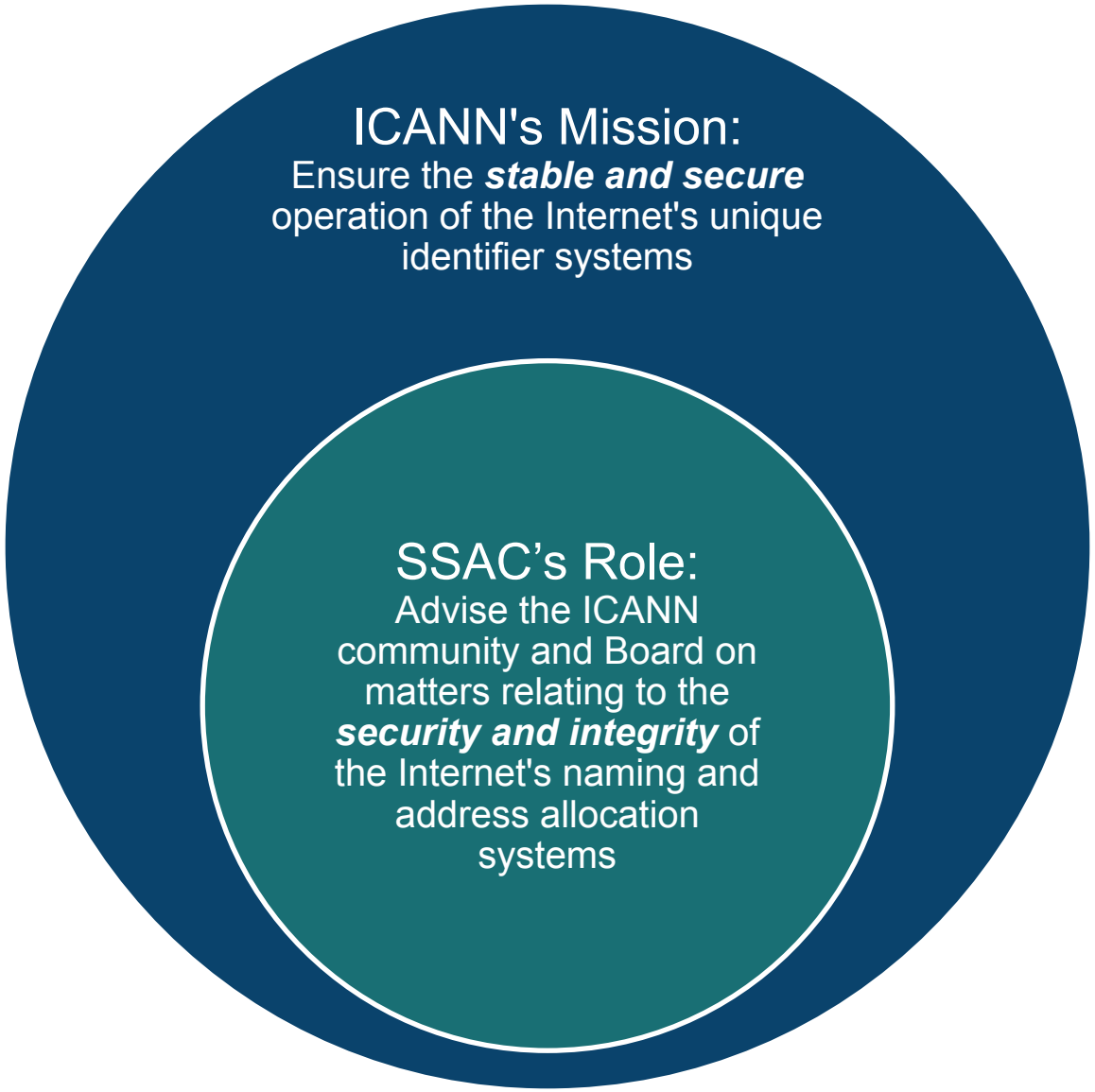
An interactive session with the ICANN Community with updates from SSAC members on current projects and future priorities

Agenda

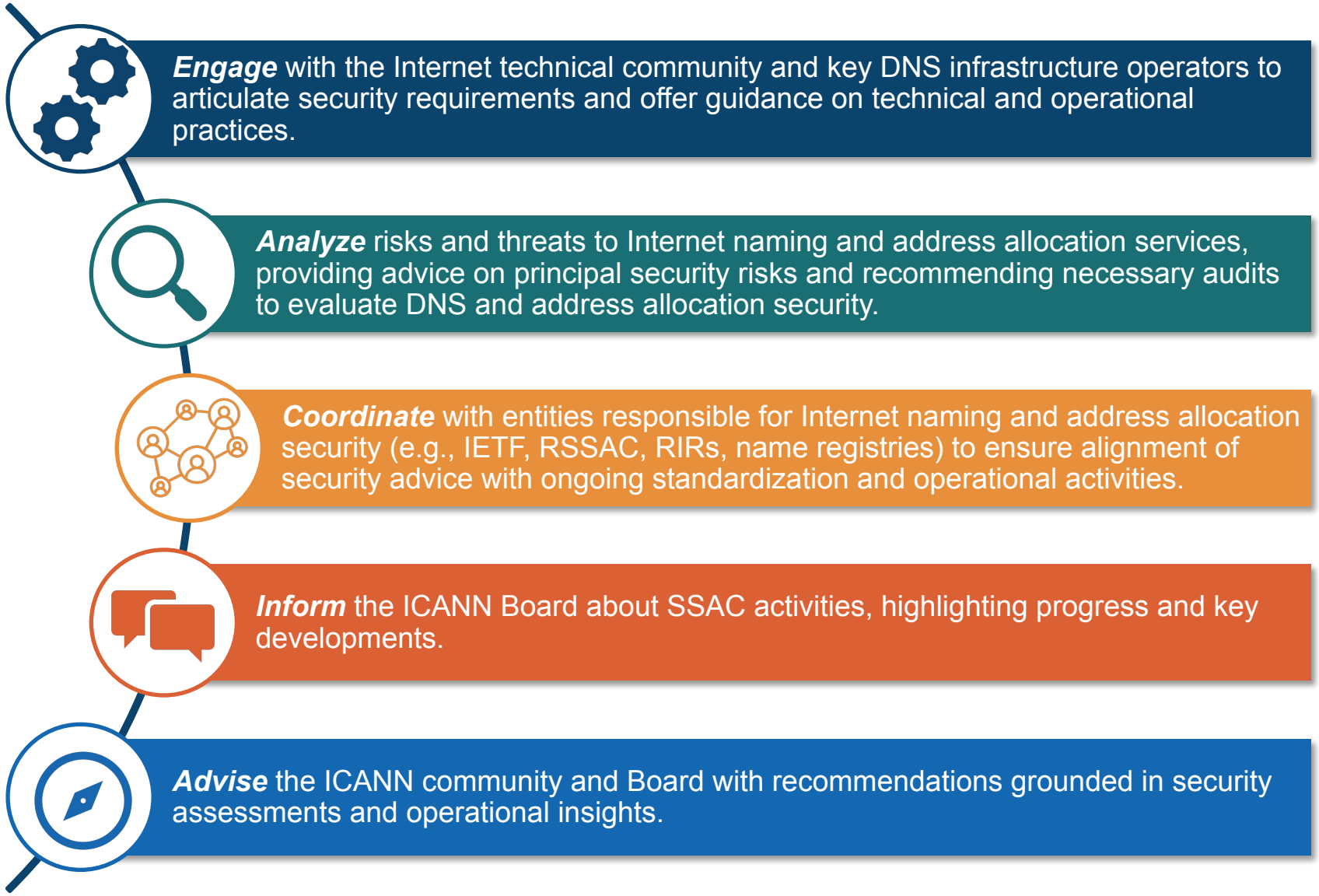
- SSAC Overview
- New Member Outreach
- SSAC's View on Name Collision Analysis Project
- DNS Abuse
- SAC123 Briefing
- Updates on Current SSAC Work Parties
- Q&A

SSAC Overview

Ram Mohan


ICANN's Mission:
Ensure the ***stable and secure*** operation of the Internet's unique identifier systems
SSAC's Role:
Advise the ICANN community and Board on matters relating to the ***security and integrity*** of the Internet's naming and address allocation systems

SSAC's Responsibilities



Engage with the Internet technical community and key DNS infrastructure operators to articulate security requirements and offer guidance on technical and operational practices.

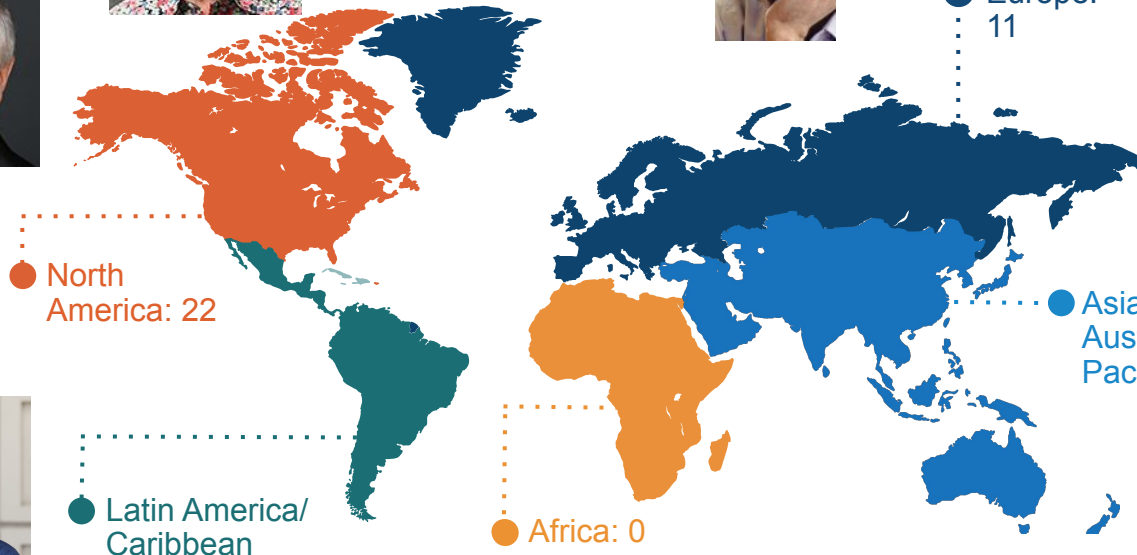
Analyze risks and threats to Internet naming and address allocation services, providing advice on principal security risks and recommending necessary audits to evaluate DNS and address allocation security.

Coordinate with entities responsible for Internet naming and address allocation security (e.g., IETF, RSSAC, RIRs, name registries) to ensure alignment of security advice with ongoing standardization and operational activities.

Inform the ICANN Board about SSAC activities, highlighting progress and key developments.

Advise the ICANN community and Board with recommendations grounded in security assessments and operational insights.

Who We Are


Europe: 11
North America: 22
Asia/ Australia/ Pacific: 4
Latin America/ Caribbean islands: 0
Africa: 0

The new SSAC Leadership Team (2024-2027)

Ram Mohan
Chair

Tara Whalen
Vice-Chair

James Galvin
ICANN Board Liaison

Jeff Bedser
Leadership Team

Barry Leiba
Leadership Team

Steve Sheng
Support Staff Lead

Danielle Rutherford
Policy Support Staff

Kathy Schnitt
Policy Support Staff

Moses Baguma
Policy Support Staff

Skills collectively include: Registry, DNS Operations, Privacy, Human Computer Interaction, Technical Standards, Risk Management, DNSSEC, Cryptography, DNS Abuse, Threat Intelligence, Internet messaging, Cybersecurity, Executive Leadership, Strategy, Public Policy, Data Analysis

Significant SSAC Publications

Domain Name System (DNS) Security:

- **DNS Response Modification:** SAC006
- **Domain Name Hijacking Report:** SAC007
- **Fast Flux Hosting and DNS:** SAC025
- **Measures to Protect Domain Registration Services:** SAC040
- **DNS Blocking / Security:** SAC050, 56, 65
- **DNS and the Internet of Things:** SAC105
- **DNS over HTTPS and DNS over TLS:** SAC109
- **DNS Abuse:** SAC115
- **Certificates:** SAC057, 74

Domain Name System (DNS) Management:

- **Global Namespace:** SAC053, 62, 66, 70, 78, 90 (Dotless domains, name collisions, public suffix list, shared use, and stability)

Registration Data:

- **WHOIS Terminology and Structure:** SAC051 **Registration Data Model:** SAC054
- **WHOIS: Blind Men and the Elephant:** SAC055

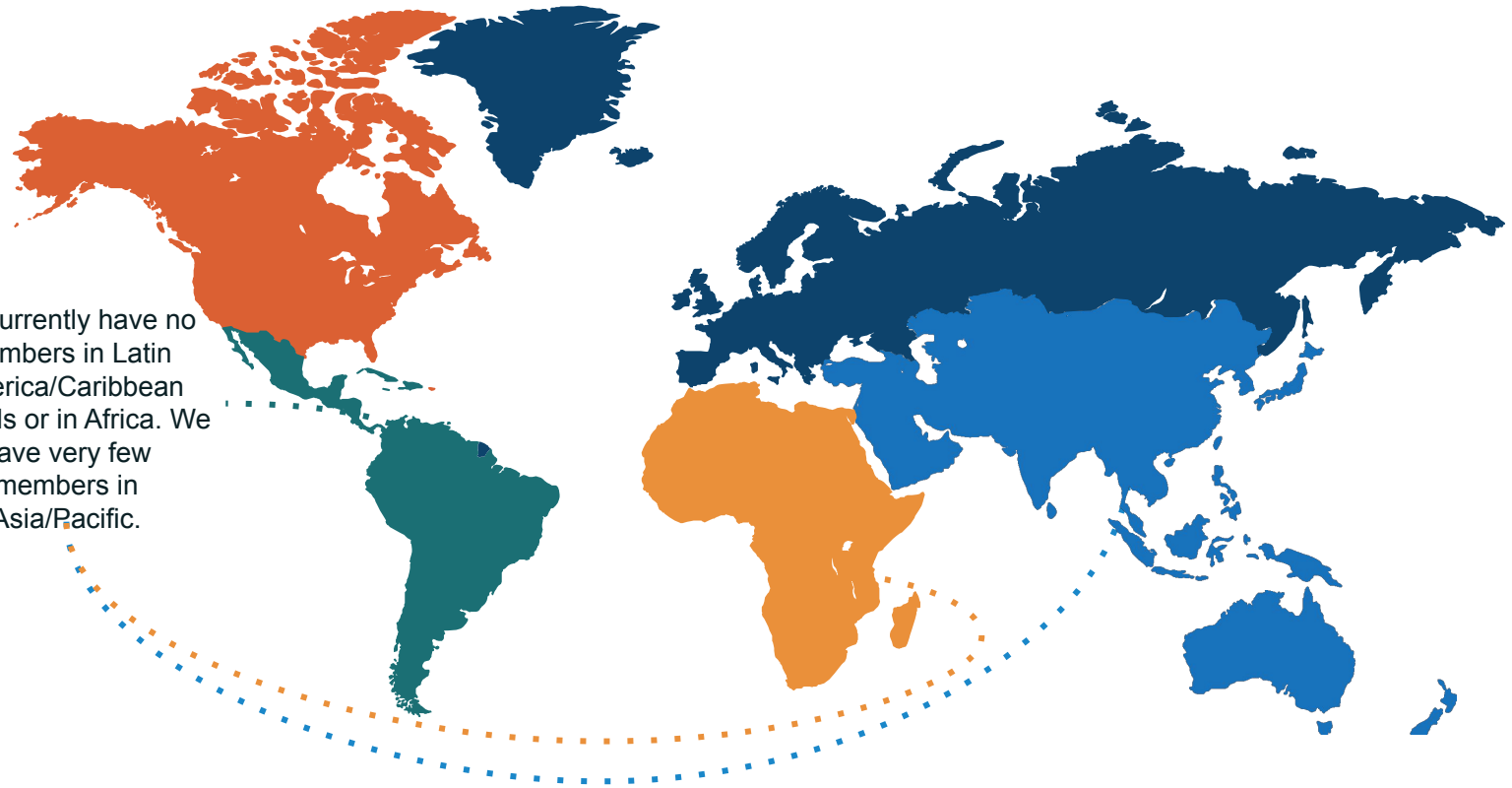
Other:

- **IDNs:** SAC084, 88, 89 (Single character TLDs, variants, ccTLD processes)
- **Routing Security:** SAC121

New Member Outreach

Tara Whalen

You can strengthen the SSAC with your unique perspective



We currently have no members in Latin America/Caribbean Islands or in Africa. We have very few members in Asia/Pacific.

- ➔ SSAC tackles crucial cybersecurity challenges for the global Internet
- ➔ We are currently short of qualified members in:
  - ◆ Africa, Latin America, and Asia-Pacific
  - ◆ Academic and research backgrounds
- ➔ We are (many) more men than women

What We Look for in New Members…

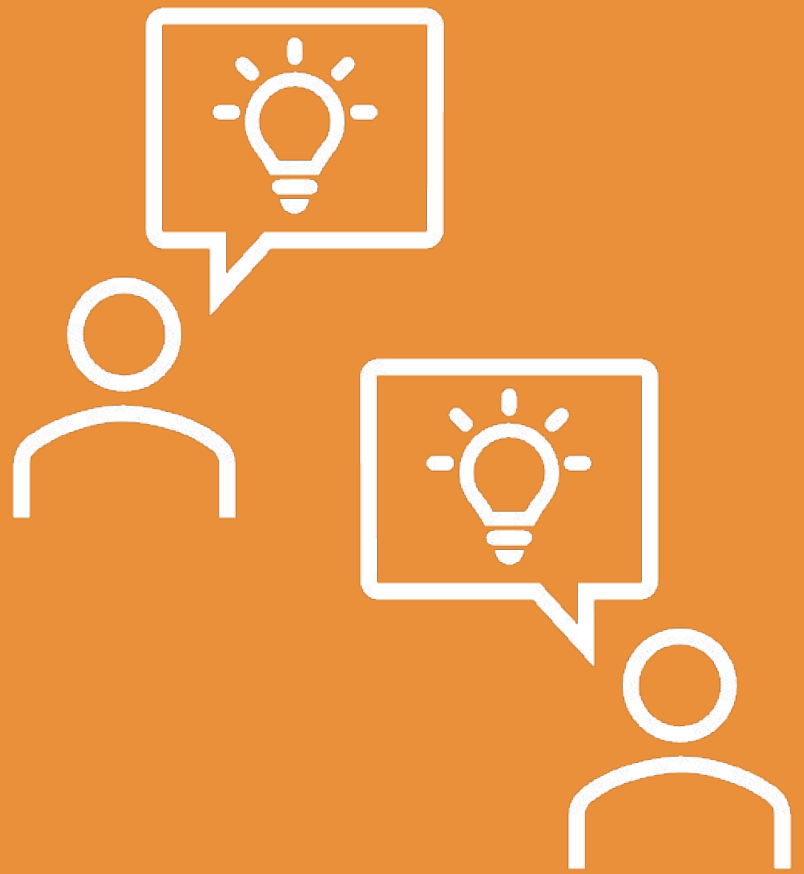
Join us and help shape the future of a secure Internet

- ***Deep engagement*** on crucial security matters
- ***Exposure*** to global security and stability topics
- ***Interaction*** with renowned security experts
- ***Career-enhancing*** research and roles
- ***International visibility*** at top security forums around the world
- ***Advise the ICANN Board*** and global DNS community
- ***Contribute directly*** to ICANN's mission
- ***Build a safer, open internet***
- ***Apply to be a member and join us in making a difference!***
  - Check out our application instructions on the SSAC website and apply here.

Come to the New SSAC Open Forum

- ➔ Informal, drop-in-style session
- ➔ Opportunity to connect directly with SSAC members
- ➔ Get insights into the committee's current projects and initiatives.
- ➔ Ask questions about becoming a member and contributing to the SSAC's mission.
- ➔ Have questions about other SSAC sessions held throughout the week? This is your chance to get them answered

➔ ***Thursday, Block 1, Room 103 B***



Name Collision Analysis Project

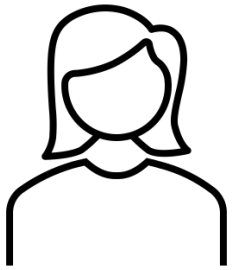
Matt Thomas and Suzanne Woolf

What Is A Name Collision?

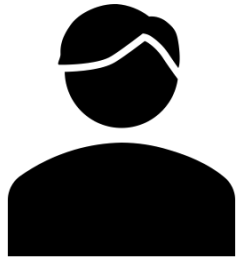
Think of domain names like house addresses.

If two houses share the same address, it becomes hard to know which one mail or deliveries should go to. There are also security issues if the mail gets delivered to the wrong address.

In the DNS, name collisions occur when a domain used in the global DNS namespace is also used in a different namespace (e.g., private enterprise), where users, software, or other functions may misinterpret it.



Home of
Danielle EndUser



Home of
Steve Networks

123 Home Ave
Example, ST USA 12345

123 Home Ave
Example, ST USA 12345

The impact of name collisions is much greater than this metaphor might suggest.

Why is Name Collision Assessment Relevant?

- **Risk of unintended consequences**. Businesses have used labels as internal TLDs in private namespaces that may leak to the global internet.
- **Introduction of new gTLDs increases probability of name collisions.** A larger pool of potential names increases the possibility that a gTLD string might unintentionally overlap with names already used in private networks or internal naming systems.
- **Measuring name collisions is difficult due to evolution of technology and network infrastructure**. Privacy enhancements in the DNS and alternative naming systems have made the DNS landscape more complex and measurements more difficult.

Why is the SSAC involved in Name Collision Studies?

- ➔ The ICANN Board wanted to ensure that gTLD delegations be done in a ***secure, stable*** and ***predictable*** manner.
- ➔ Name collisions are a factor in new gTLD delegations
- ➔ The Board tasked SSAC to conduct studies to present data, analysis and points of view, and provide
  - ◆ Specific advice regarding .home/.corp/.mail
  - ◆ General advice regarding name collisions going forward
  - ◆ Studies to be conducted in a thorough and inclusive manner

Key Takeaways from Commissioned Studies

- **Case Study of Collision Strings**
  - Potential for negative impact from name collisions has increased
  - Critical Diagnostic Measurements help predict the *impact* of name collisions
  - Leaking collision strings differ from delegated TLD queries
  - DNS service discovery protocols and search lists are a major problem

- **A Perspective Study of DNS Queries for Nonexistent Top-Level Domains**
  - Root server data itself is not enough
  - To the extent that root server data is beneficial—any root server data is sufficient
  - Similarities and differences of root server data and public recursive resolvers

- **Root Cause Analysis - New gTLD Collisions**
  - Private use of DNS suffixes (search list) is widespread
  - Name collision reports are supported strongly by measured data
  - The impact of TLD delegation ranged from *no* impact to *severe* impact

From a risk management perspective, name collisions continue to pose a persistent threat to DNS security and stability

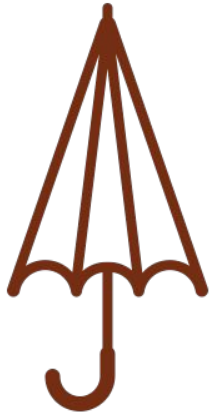
Name Collision Assessment Framework

NCAP Study 2 proposes a new **Name Collision Risk Assessment Framework** to address the documented limitations of the previous management framework.

Key Features:

- **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

Proposed Process

Stage 0: Pre-Application

Applicants encouraged to proactively assess potential name collisions by reviewing publicly available data.

Helps identify potential conflicts as early as possible.

Stage 1: Initial Risk Assessment

TRT reviews publicly available data to assess the initial risk of name collisions

If “high risk:”

- TRT submits a recommendation to the ICANN Board, OR
- Applicants may propose mitigation plan for the TRT's review

Other applications proceed to Stage 2

Stage 2: Name Collision Assessment

ICANN temporarily delegates the TLD string to the root zone.

TRT conducts one or more of the following assessments:

- No Interruption
- Controlled Interruption
- Visible Interruption
- Visible Interruption and Notification

Stage 3: Board Decision

TRT submits risk recommendation to the ICANN Board; applicant may propose mitigation plan for TRT review

ICANN Board makes the final decision on approving the application or potentially assigning the string to the Collision String List.

Technical Review Team

- We recommend establishing a highly skilled Technical Review Team to oversee the evaluation of name collision assessment.

- **TRT Member Qualifications**
  - Deep experience in *DNS management*
  - Strong understanding of *Internet infrastructure*
  - Proficient in handling historical and real-time data for *trend analysis and predictive modeling*
  - Proficient in *risk management*

- **TRT Functional Role**
  - Assess the visibility of name collisions;
  - Document data, findings, and recommendation(s);
  - Assess mitigation and remediation plan;
  - Advise on emergency response

Data Collection

You can't simply re-use the Collision detection methods you used in 2012.

- Controlled Interruption as implemented the last round doesn't work for IPv6
- Root servers & Resolver operators have much less data now than in 2012
  - ➜ Due to technology and regulatory changes

To seriously analyze name collisions, you must collect data from a variety of sources.

- Impossible to build a generalized case for root causes
- Impact assessment may require large amounts of data over significant periods of time
- ICANN org has expressed concerns about risks to privacy and confidentiality with some of the proposed data collection methods
  - ➜ These concerns need to be thoroughly understood and addressed as the DG recommendations move towards implementation.

Additional SSAC Input On Name Collisions

Ram Mohan

The SSAC Work Party has so far found strong agreement with the recommendations and observations of the NCAP Discussion Group.

High Level Input (advice in progress)

- **Name collisions continue to pose a persistent threat to DNS security and stability**
- **Data collection is crucial—the question is *when* and *where* in the evaluation process**
  - 2012 ICANN framework tagged name collision assessment and mitigation *at the end* and transferred the responsibilities (and risks) to *TLD registries*
  - Since 2012, DNS technology changes make less information available at root servers and recursive resolvers for name collision analysis; controlled interruption as implemented in 2012 does not work for IPv6 only clients
  - NCAP/SSAC proposes making name collision visible, collect data *in the beginning*, give it to the technical review team to review, and use the information to inform the granting of the TLD
- **Granting the TLD to the applicant does not resolve privacy risks related to name collision; rather, it transfers these costs and risks onto the successful applicant. The applicant may lack the capacity or incentive to properly mitigate name collision**

High Level Input (advice in progress)

- When choosing mitigation and notification methods, **ICANN's primary focus should remain on ensuring a secure and stable DNS infrastructure**, which aligns with its mission and the global internet community's interests
- Unless there are compelling privacy concerns that cannot be mitigated, the SSAC urges ICANN to prioritize finding solutions to address privacy concerns without compromising on critical security and stability aspects

Timeline

- **Estimate: 7 Apr 2024** - NCAP Discussion Group sends SSAC the Final Study 2 Report
- **Estimate: 1 May 2024** - SSAC transmits NCAP Study 2 Report and any Advice it has on name collision to ICANN Board

DNS Abuse and Impact on the Regular Internet User

Jeff Bedser

DNS Abuse and Impact on the Regular Internet user

- Board recently approved the proposed Global Amendments to the 2013 Registrar Accreditation Agreement and Base gTLD Registry Agreement
  - ➜ Specific focus on DNS Abuse and mitigation
- SSAC published SAC115: SSAC Report on an Interoperable Approach to Addressing Abuse Handling in the DNS
  - ➜ Provides actionable recommendations
- We are actively engaging with stakeholder groups across ICANN on the following questions:
  - ➜ What changes are anticipated from the new obligations?
  - ➜ The obligations specifically call out ‘disruptions’ and ‘mitigations.’ What actions could be considered that would satisfy these terms related to DNS abuse?
  - ➜ What is next for addressing the other online harms that should be mitigated outside of the ICANN contract obligations?

The Evolving Internet Name Resolution Space

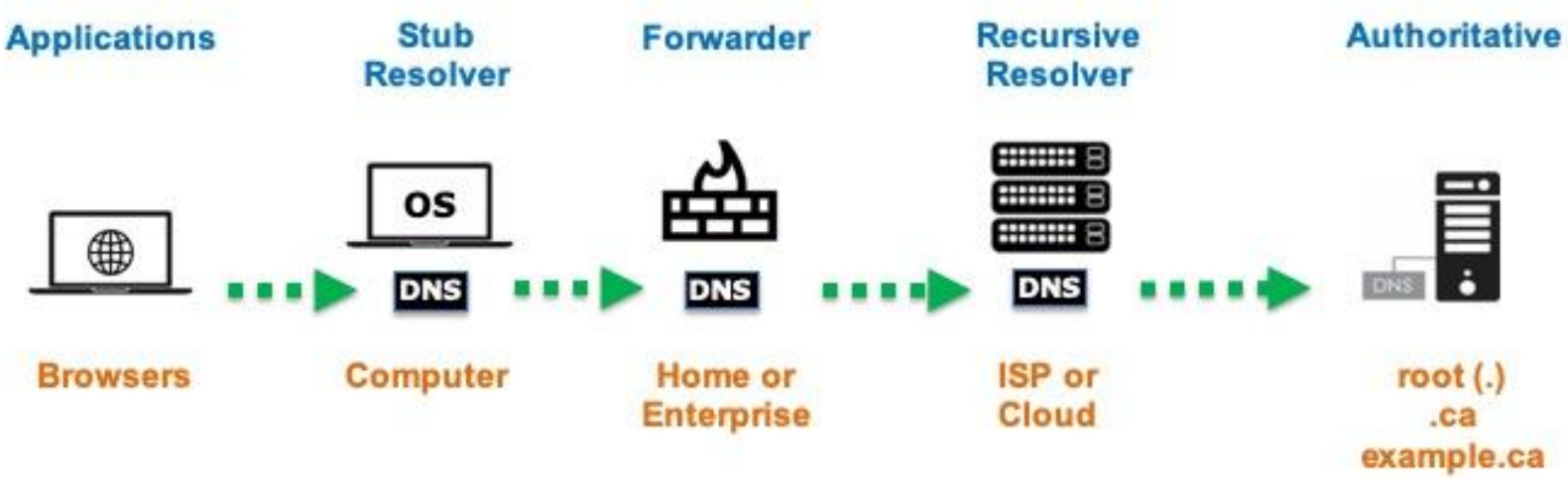
Barry Leiba

SAC123: SSAC Report on the Evolution of Internet Name Resolution

Introduction

- Names play an important role in how users trust the services they use on the Internet
- Domain name resolution is becoming more ambiguous
- Names are becoming less visible, or at least less conspicuous, to users
- Evolving needs have spurred the development of alternative naming systems with varied principles and functionalities
- This report explores the effects and implications of alternative naming systems

Traditional DNS Resolution



- DNS library is included in operating systems (OS)
- Library's operational parameters are usually automatically configured via Dynamic Host Configuration Protocol (DHCP)
- Applications rely on the OS's DNS library for name resolution, ensuring a unified method across different applications but reducing direct interaction with DNS settings

Motivations to Change Internet Name Resolution

The DNS was designed in the 1980s hierarchically within the technical constraints of that era, such as limited memory and processing power.

- Hierarchical structure facilitated ***delegated governance*** and an ***iterative name resolution process***

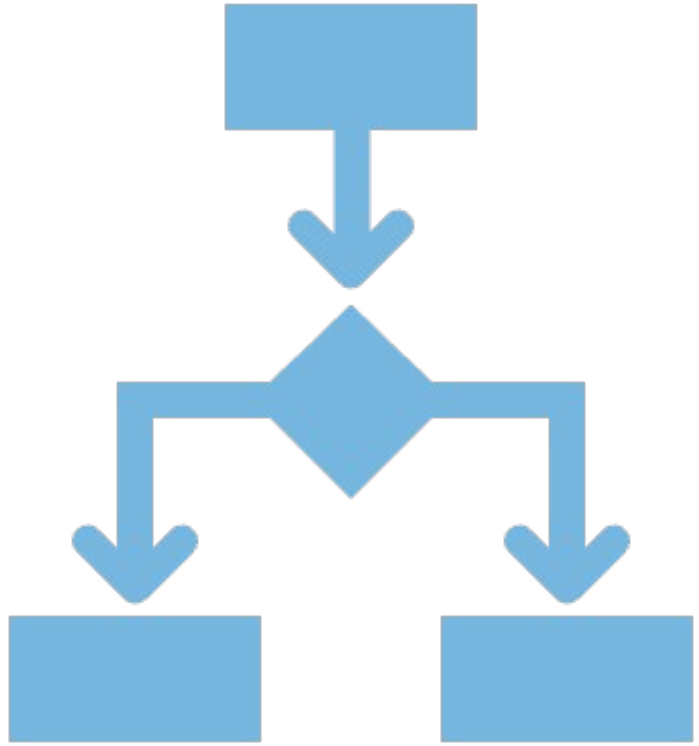
Motivations for Change:

- Speed Enhancements
- Privacy Concerns
- Authentication Enhancements
- Decentralized Governance
- Censorship Resistance

For an alternative system to gain wide acceptance, it needs to stand out in some fashion and provide functionality or overcome some technical limitation of the DNS.

Alternative Naming Systems in Use Today

- Many alt naming systems come bundled with specific applications which often bypasses administrator-controlled settings and any pre-configured DNS settings
  - ➔ Naming System: Tor
  - ➔ Application: Tor Browser
  - ➔ Context: The Tor Browser will use the Tor naming system for names ending in .ONION and the DNS for everything else
- The shift from a single, universally understood [DNS] resolution context to multiple, application-specific contexts requires users to understand the intended resolution protocol or trust the application to make the correct decision.
  - ➔ Ambiguity in Internet name resolution can give unexpected results and therefore ***undermines trust*** in the integrity of services on the Internet.



Examples of Alternative Naming Systems

Multicast DNS (.LOCAL)	• Local network resolution system using .LOCAL for device discovery without a central server • Does not use DNS protocol, not designed to interoperate with global DNS
Tor (.ONION)	• Provides anonymous service connections with non-memorable, hashed domain names • “vanity” .ONION domains can be created by users by repeatedly generating names until finding one that is memorable
Ethereum Name Service	• Based on Ethereum, a decentralized blockchain • Maps readable, dot-separated labels names like "alice.eth" to Ethereum addresses, cryptocurrency wallet addresses, and InterPlanetary File System identifiers
Unstoppable Domains	• Reservation of second-level domain names in a select set of TLDs (.888, .BITCOIN, .BLOCKCHAIN, .COIN, .CRYPTO, .DAO, .NFT, .WALLET, .X, and .ZIL.) • Built on top of the Polygon blockchain platform • Maps names to cryptocurrency wallet addresses and InterPlanetary File System identifiers
Gnu Name System	• Decentralized replacement for DNS, integrating with the GNUnet framework using a distributed hash table • Allows users to register names as top-level domains (TLDs) and resolve other namespaces within their TLDs

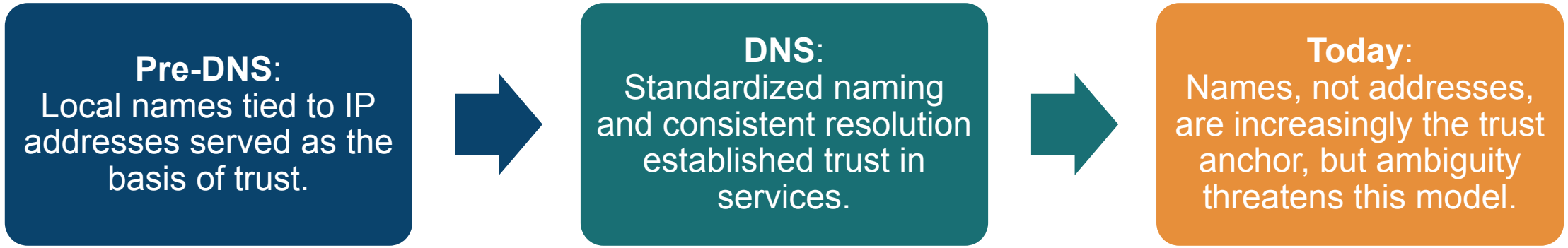
Trade-offs of Alternative Naming Systems

Naming System	Decentralized	Secure	Human Memorable
Multicast DNS (.LOCAL)	Moderate	Moderate	High
Tor (.ONION)	High	High	Low
Ethereum Name Service	High	Moderate	Moderate
Unstoppable Domains	Moderate	Moderate	High
Gnu Name System	High	High	Depends Names are either - LOW: global and not memorable, or - HIGH: not globally unique and memorable

Trends Impacting Trust and Security

- **Context**
  - ➔ Internet naming has relied on ***referential integrity***
    - Regardless of who looks up a name, the response should consistently be what the domain administrator intended
- **Emerging Trends Disrupting Referential Integrity**
  - ➔ Query-based resolution uses extra data (e.g., user location) to tailor responses, making the same query yield different results based on context.
  - ➔ Alternative naming systems utilizing similar syntax creates confusion and potential conflicts.
- **Impact**
  - ➔ Users can't be sure of the context and outcome of resolving a name
  - ➔ This ambiguity creates opportunities for misuse, where malicious actors could exploit the confusion to deceive users or redirect them to unintended destinations

Implications of Ambiguous Internet Name Resolution



- ➔ The same name can resolve differently, leading to confusion and potential encounters with malicious actors masquerading as legitimate entities (e.g., phishing)
- ➔ Users encountering resolution errors due to namespace ambiguity lack the understanding to address the problem
- ➔ Technologies like QR codes obscure domain names, hindering users' ability to identify the true destination of a link

The combination of ambiguous resolution and reduced name visibility significantly undermines user confidence and trust in online services

Proposals to Facilitate Namespace Coordination

.INTERNAL

- SAC113
- Proposes reserving a portion of the namespace for private, internal DNS uses.

.ALT

- RFC 9476
- Proposes the .alt top-level domain for alternative naming systems

➔ Both proposals are ***voluntary*** and ***non-intrusive***

➔ They do not enforce usage but encourage good practices to ***minimize ambiguity***

➔ Widespread adoption could significantly mitigate namespace ambiguity and ***enhance online trust***

SSAC Recommendations

ICANN should **track and provide regular updates** on:

1. Alternative protocols that make use of the domain namespace, and
2. Efforts to create mitigations and reduce risks inherent in the coexistence of multiple namespaces and protocols.

ICANN should keep the ICANN community abreast of new developments through such means as the Emerging Identifier Technologies panels.

Work Party: DNSSEC DS Automation

Peter Thomassen & Steve Crocker

Current State of DNSSEC DS Automation

- ➔ Registries and registrars play a critical role in the DNSSEC ecosystem
  - Their internal DNSSEC operations are mostly automated today

- ➔ However, DS record provisioning remains largely manual when the child uses a third-party DNS service

- ➔ About 10 ccTLDs / 2 registrars / 1 RIR maintain DS records automatically

Challenges and Opportunities in DS Record Automation

Why Automation Matters

Security and Stability: Manual updates are error-prone, increasing the risk of vulnerabilities and jeopardizing the integrity of the DNS.

Operational Efficiency: Automation streamlines operations, saving time and resources for both registrars and registries.

Limited Adoption: Lack of standards, compatibility issues, and potential hesitancy towards new technologies hinder wider adoption.

Bridging the Gap

The SSAC is working on a report to ***encourage*** the creation of industry best practices for DS automation.

ICANN Org and gTLD leaders should study how to ***support*** and ***incentivize*** DS automation within their communities.

Work Party: Registrar Nameserver Management

kc claffy & Gautam Akiwate

Registar NS Management - Problem Statement

- **Challenge:** Difficulty managing expired domain names creates a security risk for the DNS
- **Risk:** Creates a new attack surface for malicious actors to hijack domain resolution for dependent domains
- **Contributing Factors:**
  - ➜ Technical Requirement: RFC 1034 mandates at least two name servers for any domain, hindering deletion of expired domains with dependencies.
  - ➜ Policy Restrictions: Preventing orphan glue records further complicates domain deletion.
  - ➜ Registrar Incentive: Sponsoring expired domains is burdensome for registrars, incentivizing workarounds like creating sacrificial nameservers.
- **Impact:** Over the last 9 years: > 512K domains have been implicitly exposed to domain resolution hijacking

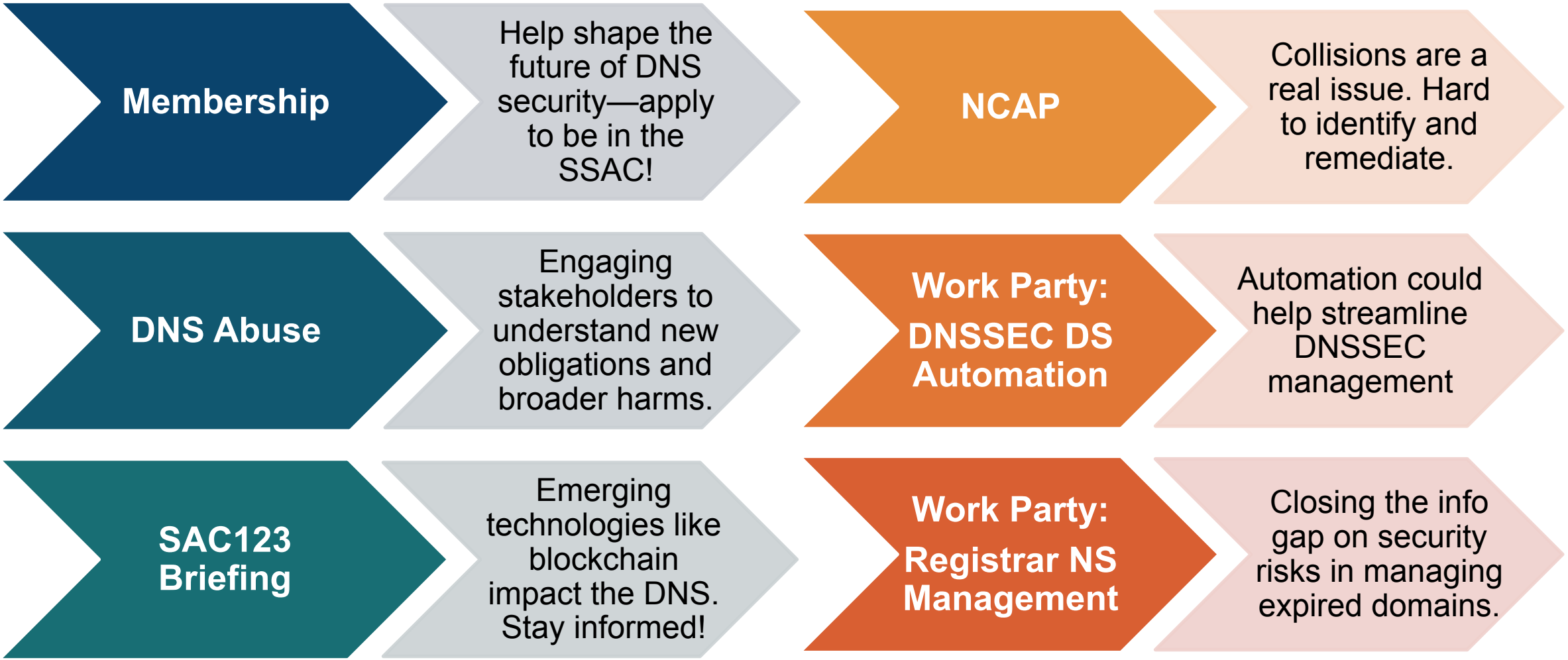
Registar NS Management - Scope

- Building on the risks identified in the paper ***Risky BIZness: Risks Derived from Registrar Name Management***
- SSAC is 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

Summary

Ram Mohan

Summary


Membership
Help shape the future of DNS security—apply to be in the SSAC!
NCAP
Collisions are a real issue. Hard to identify and remediate.
DNS Abuse
Engaging stakeholders to understand new obligations and broader harms.
Work Party: DNSSEC DS Automation
Automation could help streamline DNSSEC management
SAC123 Briefing
Emerging technologies like blockchain impact the DNS. Stay informed!
Work Party: Registrar NS Management
Closing the info gap on security risks in managing expired domains.