SSAC Activities Update

Rod Rasmussen, SSAC Chair | ICANN71 | June 2021

Agenda 1 Slide

1. SSAC Overview
2. SAC115: SSAC Report on an Interoperable Approach to Addressing Abuse Handling in the DNS
3. Name Collision Analysis Project
4. Current SSAC Work Parties
5. SSAC Skills and Potential New Member Outreach
6. Q&A

Security and Stability Advisory Committee (SSAC)

Who We Are

- **33** 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

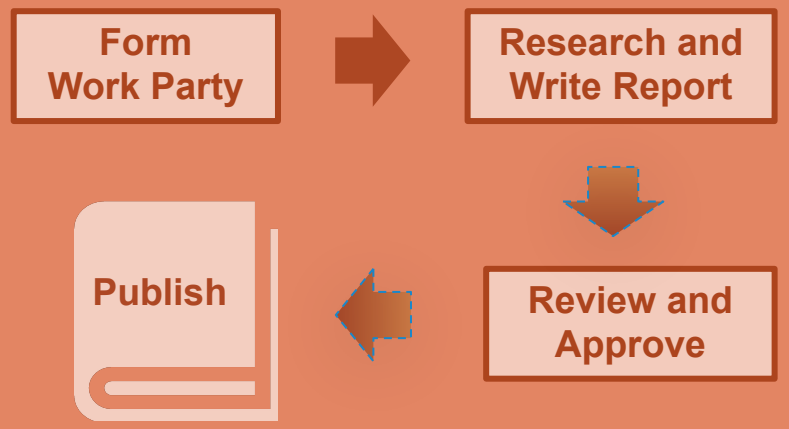
116 Publications since 2002

Security and Stability Advisory Committee (SSAC)

ICANN's Mission & Commitments

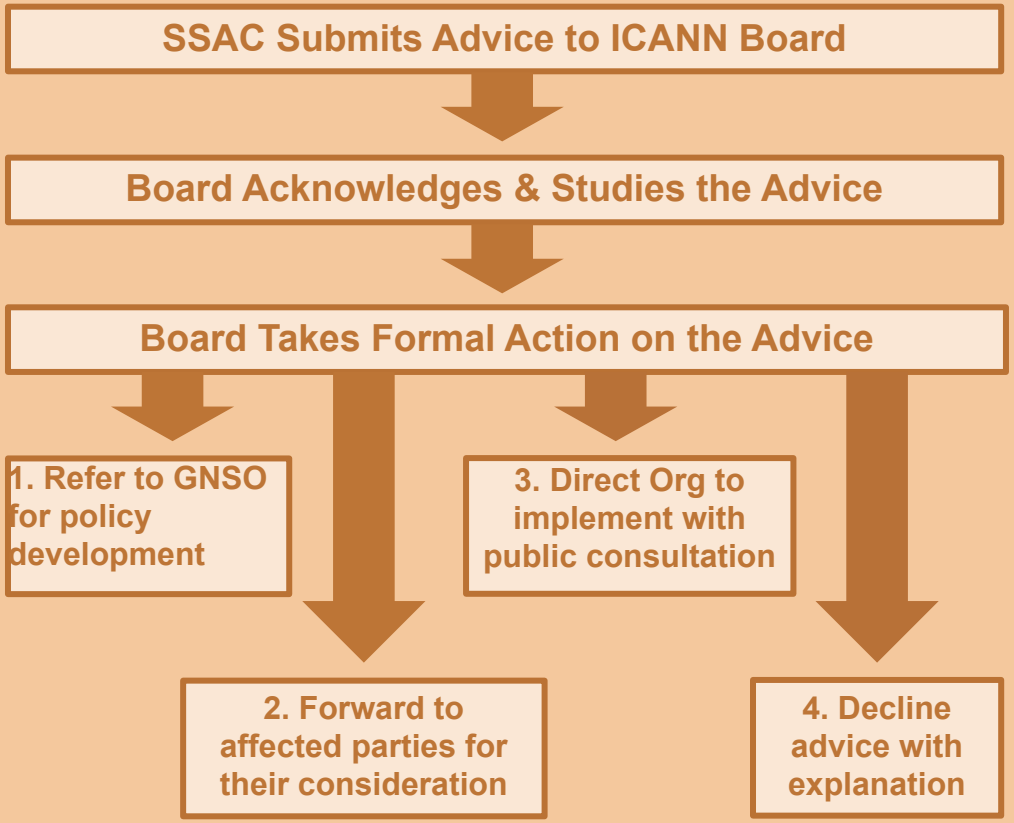
- Ensure the stable and secure operation of the Internet's unique identifier systems.
- Preserve and enhance the administration of the DNS and the operational stability, reliability, security, global interoperability, resilience, and openness of the DNS and the Internet.

SSAC Publication Process



Consideration of SSAC Advice

(to the ICANN Board)



Security and Stability Advisory Committee (SSAC)

Recent Publications

[SAC116]: SSAC Comments on the Second Security, Stability, and Resiliency (SSR2) Review Team Final Report

[SAC115]: SSAC Report on an Interoperable Approach to Addressing Abuse Handling in the DNS

[SAC114]: Comments on the GNSO New gTLD Subsequent Procedures Draft Final Report

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

SAC115: SSAC Report on an Interoperable Approach to Addressing Abuse Handling in the DNS

Jeff Bedser

Scope and purpose of report

Purpose of report

Goal: Reduce victimization of Internet users

Strategy: Interoperable approach based on universal standards for DNS abuse handling

Desired Outcome: SAC115 acts as a catalyst to channel ongoing efforts in order to begin establishing universal standards

Defining the problem

Defining the problem

DNS abuse in SAC115 refers to the use of domain names or the DNS to perpetuate abusive activities. The report does not define "DNS Abuse" but points to definitions commonly used in the ICANN Community.

ICANN Community Recognized DNS Abuses

- **Malware**
- **Botnets**
- **Phishing**
- **Pharming**
- **Spam***

- Many other forms of DNS abuse exist, are reported, and are acted upon by service providers
- New types of abuse are commonly created, and their frequency waxes and wanes over time
- No individual list of abuse types will ever be comprehensive
- The SSAC supports the concept of regular, community-driven review of DNS abuse definitions

Defining the problem

What are we doing about DNS abuse?

Blocking and filtering

- Quick to implement
- Difficult to maintain at scale
- High number of false positives
- Blacklists go stale
- Possibility of collateral damage

Notification and take down

- May take a long time
- Inconsistent outcomes
- Possibility of collateral damage

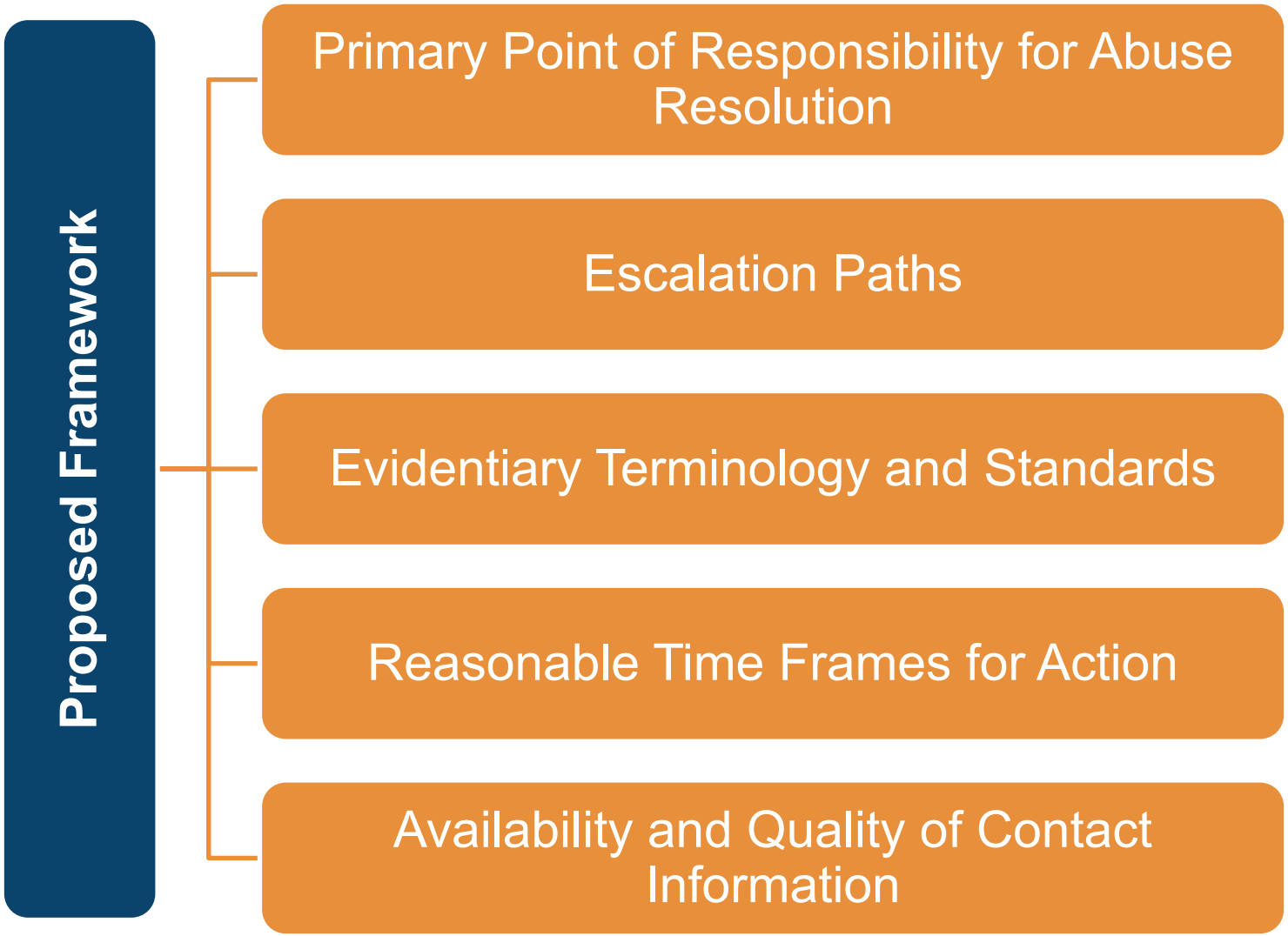
Leading efforts

- APWG
- M3AAWG
- FIRST
- Internet & Jurisdiction Policy Network
- Cybersecurity Tech Accord
- PIR DNS Abuse Institute
- Digital Trust and Safety Partnership

Notifier Programs

- Expedite DNS abuse remediation
- Explicit network of trust
- Scaling is difficult by its nature
- Each program sets its own definitions and standards

Framework for interoperable approach


Proposed Framework
Primary Point of Responsibility for Abuse Resolution
Escalation Paths
Evidentiary Terminology and Standards
Reasonable Time Frames for Action
Availability and Quality of Contact Information

Primary Point of Responsibility for Abuse Resolution

Principle: Each incident of DNS abuse should have a reporting entry point in the DNS ecosystem where that abuse is resolved by policy and process

Manifestation of Abuse	Primary Party	Secondary & Escalation Parties
Domain name registered to perpetuate abuse	Registrar for domain	Registry for domain Web host for web content Email provider for spam accounts ISP for abusive activity
Domain name registered to perpetuate abuse (Registry operator policy exists to receive abuse complaints)	Registrar and Registry operator	Web host for web content Email provider for spam accounts ISP for abusive activity
Website compromised for abuse	Owner of domain name Hosting provider	Registrar of domain (for contacts)
Account on major Internet platform	Platform service provider	

Escalation Paths

Principle: When a reporter either reports to the wrong party or does not get a response, there needs to be a documented and actionable escalation path to assist in mitigating the abuse.

- Evidence of both the abuse and the time of report can be conveyed to the next party in the escalation path
- Standardized paths will allow for eventual automation
- SAC115 does not include proposed escalation paths beyond Appendix B
- Escalation paths and standardized documentation should be determined by stakeholders

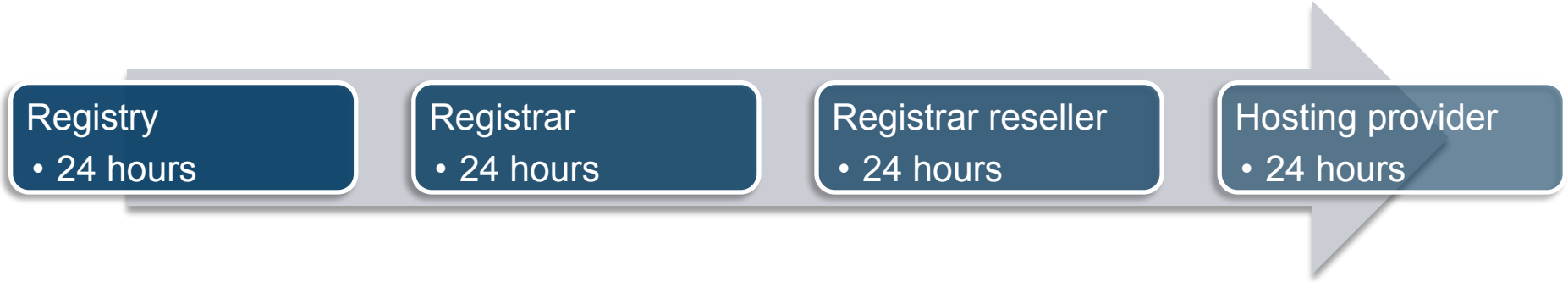
Evidentiary Terminology and Standards

Principle: Reporters of abuse have the responsibility of providing evidence and documentation. Setting objective standards of evidence to support action will enhance transparency and accountability for service providers.

Temporal Relevance	Visual	Behavioral	Demonstrative
When did it happen?	Was there an "A" or "AAAA" DNS record logged for the domain?	Are there logs of activities regarding the domain name itself?	What is the abuse for which the domain was used?
How long after the registration did the abuse occur?	Was there content hosted on the domain that was not a parked page record and that was captured via screenshot or other means?	Records in the zone? Changes in delegations? WHOIS records? Passive DNS?	How did it violate ToS that supports rapid action?
How long after the abuse was detected did the evidence get logged or captured?			What is the impact of abuse?
			What are the anti-abuse policies of the responsible party?

Reasonable Time Frames for Action

Principle: The timely mitigation of DNS abuse is extremely important to minimize victimization of the abuse.



- **Escalations:** maximum time for escalation and remediation should be no longer than 96 hours
- **Expedited escalations:** escalation and remediation of urgent requests should be commensurate with the potential harm threatened

Availability and Quality of Contact Information

Principle: Accurate, thorough, and accessible contact information for entities in the DNS ecosystem is critical to establishing escalation paths and mitigating abuse.

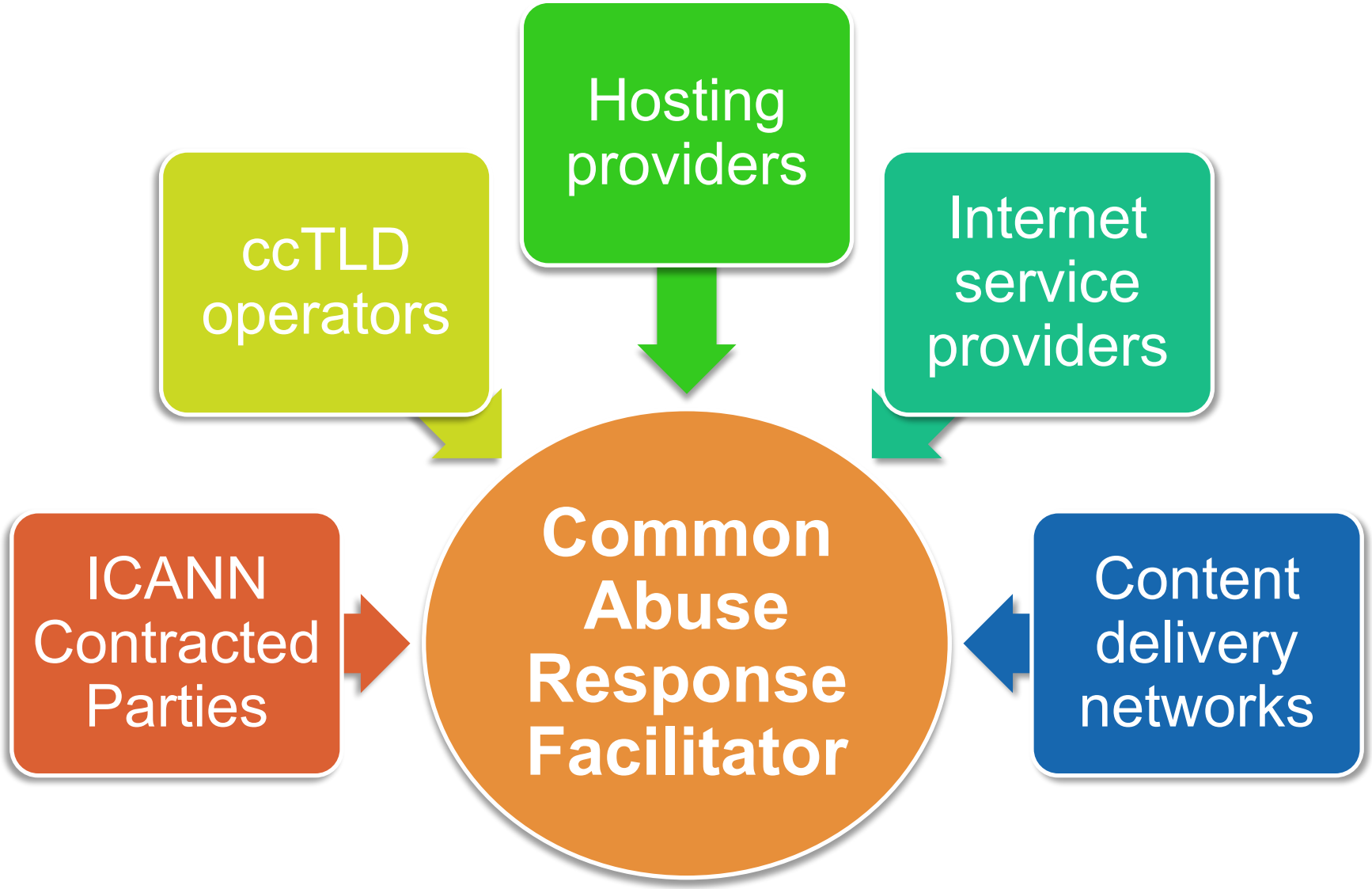
- Readily accessible contact information becomes increasingly difficult to find the further downstream from the registry
- Uncertainty incentivizes reporting parties to use a ‘scattergun approach’
- Possible solution is to create a single point of contact determination where a reporter can identify the type of abuse and get directed to appropriate parties

Findings

Findings

Lack of coordination leads to inconsistent approaches to DNS abuse management

Opportunity for a Common Abuse Response Facilitator


Hosting providers
ccTLD operators
Internet service providers
ICANN Contracted Parties
Common Abuse Response Facilitator
Content delivery networks

Common Abuse Response Facilitator's Mission

- Scope the problem space
- Convene relevant stakeholders
- Implement "best practices model"
- Create evidentiary standards
- Execute a common abuse handling framework
- Develop abuse reporting approach that includes the elements in SAC115
- Establish standardized methodologies to build trust in abuse reports
- Report regularly on the effectiveness of the Facilitator's programs

Recommendation

Recommendation

Recommendation 1: The SSAC recommends that the ICANN community continue to work together with the extended DNS infrastructure community in an effort to

(1) examine and refine the proposal for a Common Abuse Response Facilitator to be created to streamline abuse reporting and minimize abuse victimization; and

(2) define the role and scope of work for the Common Abuse Response Facilitator, using SAC115 as an input.

Name Collision Analysis Project

James Galvin, Patrik Fältström, Matthew Thomas
(NCAP Co-Chairs)

Our Work In 5 Tasks

1. Root cause analysis
2. Additional data collection
3. Answering board questions
4. Case study of .corp, .home, .mail, .lan, .local, .internal
5. Name collision analysis

Root Cause Analysis

- Work to be done by Technical Investigator
- There are 40+ reports that ICANN has received since 2012 round
- ICANN will approach reporters to confirm participation
- Work product to be delivered to discussion group
- Work product is needed in advance of Study 3

Additional Data Collection

- Review and state questions for other data sources
- Identify other data sources
- Will send questions to identified sources
- Responses to be provided to discussion group
- Work product is needed for name collision analysis (Task 5)

Answering Board Questions

- Template for answering each question
- Separate draft document for each question

Case Study of .corp, .home, .mail, .lan, .local, .internal

- John Kristoff (Research Fellow) and Steve Sheng will be creating first draft

Name Collision Analysis

- An essential deliverable from us
  - What process will we recommend the board use for considering the presence of name collisions when evaluating future applications?
  - Framework under development as a starting point for discussion group
- Data sensitivity analysis is part of this work
  - No decision yet on whether this is part of the final work product or a separate document
- Research fellow currently reviewing prior meetings to ensure we have captured all open questions
- Focused work will wait until we have our case study work product

Next Steps

- Research fellow
  - Capturing questions from prior meetings
  - Briefing document of all presentations to date
  - Drafting case study
- Technical Investigator
  - Root cause analysis
- Discussion group
  - Questions for data collection
  - Responding to board questions
- Data collection

Current SSAC Work Parties

Current Work Parties

- Name Collision Analysis Project
- DNS Abuse
- Routing Security
- Root Service Early Warning System
- EPDP Phase 2a (Ongoing)
- Registration Transfer Policy Review (TPR)
- Scan of Threats to Internet Naming and Addressing (Ongoing)
- Reviewing Community Feedback on SAC114 [SubPro]
- Tracking SSAC Advice to the Board (Ongoing)
- DNSSEC and Security Workshops (Ongoing)
- Membership Committee (Ongoing)

Routing Security

- The scope is to examine the security and stability implications of insecurities in the Internet's routing system, and best ways network operators can address them
- The initial publication will provide a high level overview of
  - The Internet's routing system
  - Implications of incorrect route announcements
  - The role of network operators in securing the Internet's routing system
  - The size and urgency of routing security issues
- The initial focus is on the security and stability implications of routing incidents for the DNS and DNS operators
- What would you like to know about routing incidents and their impact on the DNS?
  - Contact us!
  - Send an email to ssac-staff@icann.org

Root Service Early Warning System

- The SSAC has chartered a work party to comment on OCTO-15: Recommendations for Early Warning for Root Zone Scaling and explore the possibility of a root service early warning system (EWS)
- This work party's tasks included:
  - Reviewing all past material on the topic
  - Questioning the assumptions inherent in OCTO-15
  - Commenting on the feasibility, desirability, practicality and usefulness of a root service EWS
  - Reviewing developments in the DNS and root service, that could affect overall stability of the root service, including such developments as deployments of new technologies and changes to the overall DNS ecosystem

EPDP Phase 2A - Legal and Natural Persons

SSAC Work Party View:

- The distinction between legal and natural persons is an approximate proxy for whether data may be publicly disclosed
- Use explicit declarations and clear and explicit guidance
- Use a third status, “Unknown” to cover both existing registrations and new registrations where the answer is indeterminate.
- Consider extensibility in registrant data model to accommodate future requirements
- Report on the number of Unknown registrations and gradually reduce the number
- Permit registrars to fold these requirements into their business process efficiently as long as the registrant is well informed and has appropriate choices
- All of the above is consistent with maximum disclosure and the expected use of differentiated access to support security research and other authorized uses

Registration Transfer Policy Review (TPR)

- SSAC involvement as invited subject matter expert
- Main focus of WG is consideration of auth code and loss of access to contact details
- We have raised the question of smooth transition of DNS operation, both signed and unsigned.

SSAC Organizational Review Implementation

- On 17 December 2018, the Independent Examiner (Analysis Group) published their Final Report on the 2nd SSAC Review
- On May 27, 2019, the SSAC published the Feasibility Assessment and Initial Implementation Plan (FAIIP) as SSAC2019-04
- On 12 March 2020, the SSAC's Detailed Implementation Plan based on the FAIIP was accepted by the Board
- Implementation updates were provided throughout 2020
- On 3 December 2020, the SSAC update stated that it considers that all recommendations approved by the Board have now been either completed, or integrated into ongoing SSAC processes, as documented in the SSAC Operational Procedures and proposed that implementation be recorded as complete.
- The 3 December SSAC Implementation Update (SSAC2020-13) was considered by the Board Operational Effectiveness Committee in January 2021 and was accepted by the Board in March 2021 and is now considered complete

Threats to Internet Naming and Addressing

- SSAC initiated an environmental scan of threats and risks to the DNS in the following categories:
  - DNS Security: Protocol, infrastructure, namespace
  - Domain Name Abuse
  - Addressing and Routing
  - Registration Services
- SSAC is using its threat identification, assessment, and ranking exercise to inform future work parties and membership recruitment efforts
- SSAC shared its findings with the ICANN Board Technical Committee and is engaging in ongoing discussions

Topics of Interest/Possible New Work

- Evolution of DNS Resolution
  - Alternative protocols
  - Resolverless DNS
  - Operational concentration of the DNS infrastructure
- DNSSEC DS key management and other registrar/registry control issues
- Concerns of overloading HTTPS for other privacy issues
- Examining datasets available from ICANN for use in the investigation of SSR-related issues that fall within SSAC's remit
- Examining practices that can potentially expose registrants to domain name hijacking via lame delegations
- Forced removal or transfer of a ccTLD

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
  - Registrar Operations
  - Browser Development/Testing
  - Mobile Apps Development/Testing
  - Low bandwidth resource constrained Internet connectivity
  - Red Team experience
  - Risk management
  - Law Enforcement experience
- The SSAC is interested in increasing membership from Africa, Latin America, and Asia-Pacific

SSAC Contact for Potential New Members

- Individuals who are interested in enquiring about SSAC membership should:
  - Contact Rod or Julie,
  - Contact any member of SSAC Support Staff, or
  - Send an email to ssac-staff@icann.org

Questions to the Community

- What topics would you like SSAC to consider as work items?
- What would you like SSAC to comment on?

Thank you