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

Rod Rasmussen, Chair, Security and Stability Advisory Committee (SSAC)

20 May 2021

Agenda

- Scope and purpose of report
- Defining the problem
- Framework for interoperable approach
- Findings
- Recommendation

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

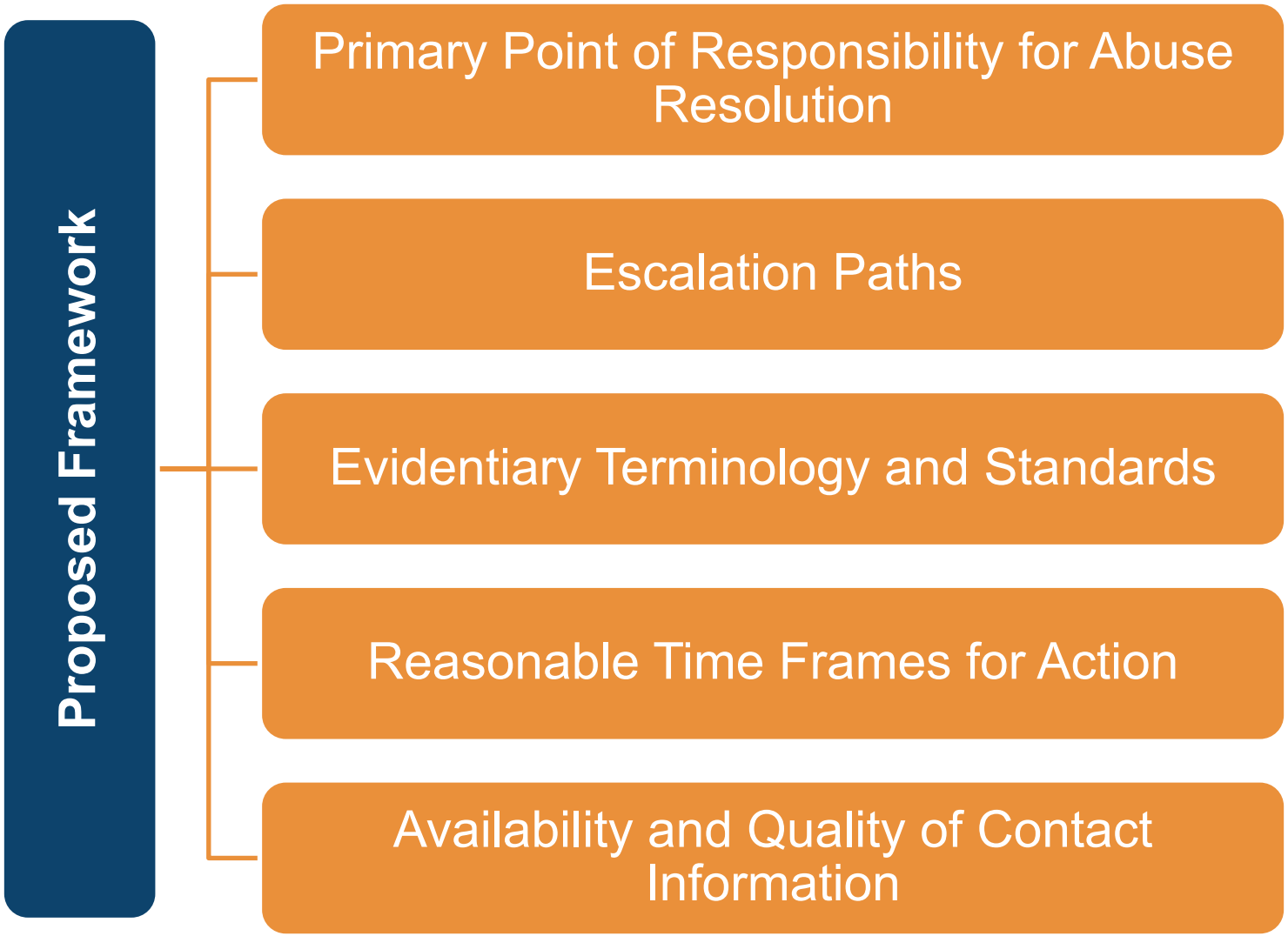
Leading efforts

- 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	

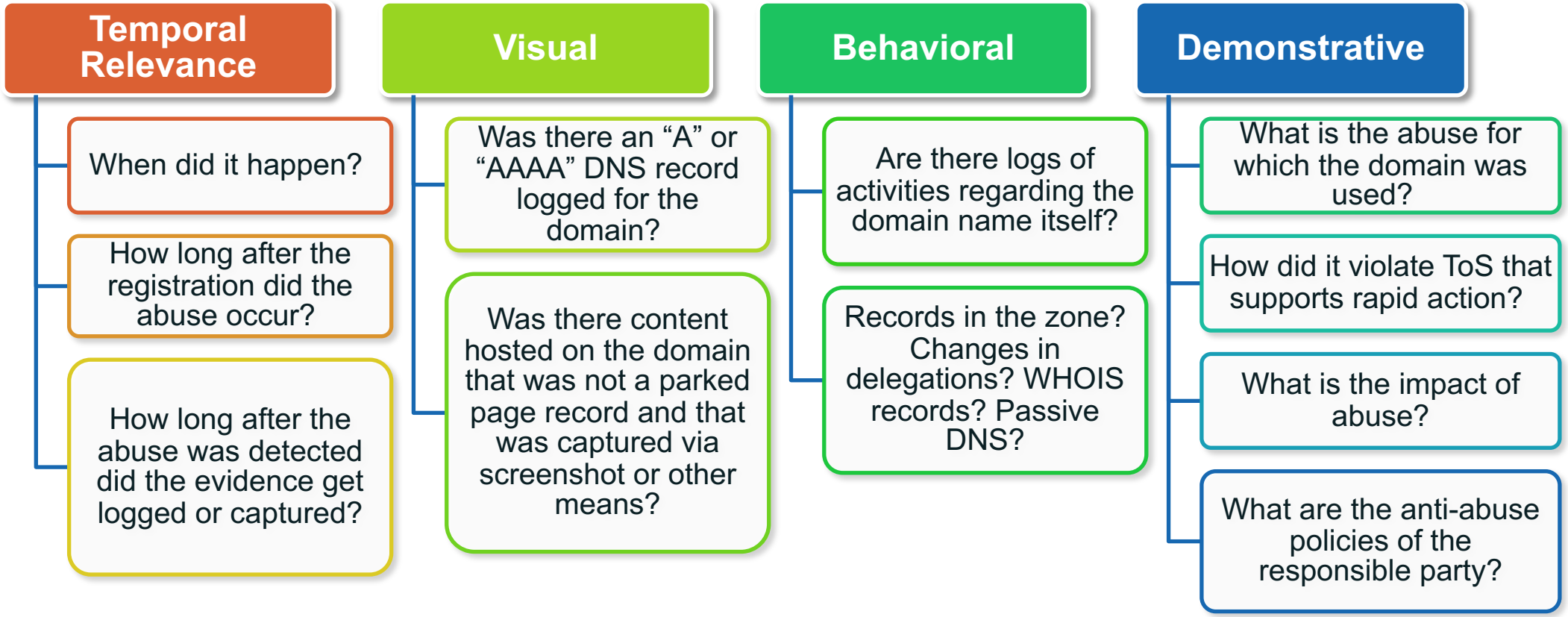
Escalation Paths

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

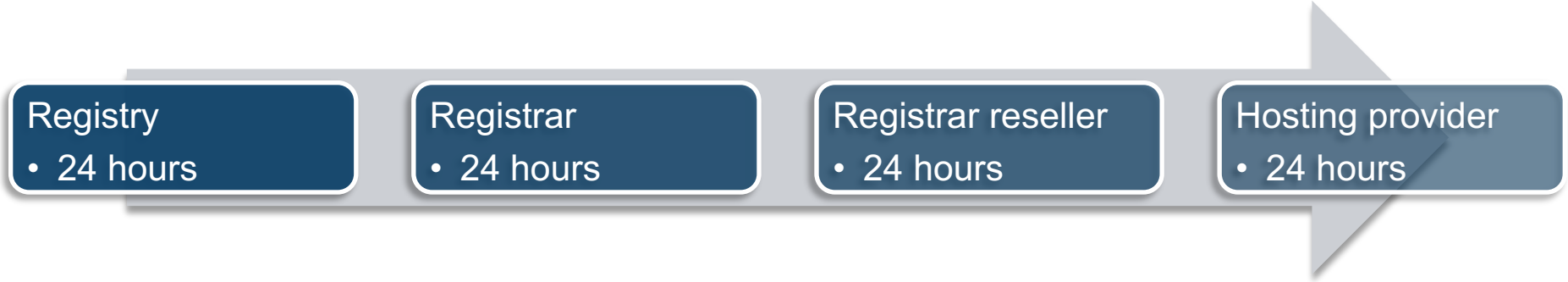
Evidentiary Terminology and Standards

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.



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

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.

Discussion