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

A Report from the ICANN Security and Stability Advisory Committee (SSAC)

19 March 2021

Preface

This is a report to the ICANN Board, the ICANN organization (ICANN org), the ICANN community, and, more broadly, the Internet community from the ICANN Security and Stability Advisory Committee (SSAC) about the abuse of domain names.

The SSAC focuses on matters relating to the security and integrity of the Internet's naming and address allocation systems. This includes operational matters (e.g., pertaining to the correct and reliable operation of the root zone publication system), technical administration matters (e.g., pertaining to address allocation and Internet number assignment), and registration matters (e.g., pertaining to registry and registrar services). SSAC engages in ongoing threat assessment and risk analysis of the Internet naming and address allocation services to assess where the principal threats to stability and security lie, and advises the ICANN community accordingly. The SSAC has no authority to regulate, enforce, or adjudicate. Those functions belong to other parties, and the advice offered here should be evaluated on its merits.

Table of Contents

Executive Summary

Much of the success of the Internet comes from its architecture as a "network of networks," where operators and users of home, corporate, government, or public networks make their own decisions about technical and policy characteristics of those networks, but they also connect voluntarily to other networks because there's shared benefit in doing so. It's in their mutual interests to retain their autonomy, but also to support technical protocols and operational rules that allow them to easily interoperate. This balance of independence and cooperation allows them to work together where it's helpful, but doesn't require centralized control over them. This report intends to demonstrate that addressing abuses of the domain name system (DNS) could and should be handled in a similar fashion.

There are many ways to define the term “DNS Abuse” including, abuse of the protocol itself, abuse of the DNS infrastructure, using the DNS as a supporting service for some other abuse, and the use of domain names themselves in an abusive manner. In this report, the SSAC focuses on cases where domain names themselves are used in an abusive manner. These are often colloquially referred to within the ICANN community as “technical abuses”, which generally refer to abuses spelled out in ICANN’s registry agreements in Specification 11.3 (b)[1] and that have been the focus of many community discussions from 2018-2020.[2] In general, the term “DNS abuse” in this report refers to the *use* of domain names, or the DNS system, to perpetuate abusive activities. Abuse on the Internet continues to victimize millions annually,[3,4] reducing trust in the Internet, including the DNS, as a place to conduct commercial and non-commercial activities. This erosion of trust negatively impacts all parties in the Internet ecosystem, from end-users to infrastructure service providers.

In this report, the SSAC proposes a general framework of best practices and processes to streamline reporting DNS abuse and abuse on the Internet in general. This effort is focused on determining approaches and methodologies that could ultimately reduce the severity and duration of victimization for end-users. This report focuses on one specific area of the DNS abuse lifecycle, namely abuse handling. Other topics in the space, including, but not limited to, prevention, mitigation methods, and education may be explored in future SSAC work. This report is intended to be of benefit to the victims of DNS abuse, reporters of DNS abuse, and to those responsible for identifying and remediating DNS abuse.

---

[1] See ICANN Registry Agreement, https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-09jan14-en.htm

[2] ICANN organization has had descriptions and working definitions of ‘DNS abuse’ and related terms integrated with its activities for over a decade, including (but not limited to) ICANN org’s Security, Stability, and Resiliency Frameworks from 2009 to 2017, the ICANN’s consensus community findings in the New gTLD Program as well as subsequent consensus on safeguards, the 2013 Specification 11b contractual obligation which enumerates abusive activities, and ICANN’s own DNS Abuse Activity Reporting Project (DAAR).

[3] See 2019 Internet Crime Report Released, https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120

[4] See Internet Organised Crime Threat Assessment (IOCTA) 2019, https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019

Outlined below are the elements of this framework and recommended next steps to see it taken up by the ICANN and the larger Internet-wide communities, including:

1. encourage standard definitions of abuse (see Section 2);
2. encourage 'notifier programs' that will expedite and make more efficient abuse handling in certain parts of the ecosystem (see Section 2.8.1);
3. determine the appropriate primary point of responsibility for abuse resolution (see Section 3);
4. identify best practices for deployment of evidentiary standards (see Section 4);
5. establish standardized escalation paths for abuse resolution (see Section 5);
6. determine reasonable timeframes for action on abuse reports (see Section 6); and
7. create a single point of contact determination whereby a reporter can identify the type of abuse and get directed to appropriate parties (see Section 7)

While the SSAC acknowledges the opportunity and need to create the anti-abuse efforts outlined in this report, it is not advocating for any particular organization or entity to fulfill them. The SSAC does anticipate, however, that ICANN org and the ICANN community will continue to fulfill their role to encourage unified community-led efforts. To that end, we make the following 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.

1 Introduction

This report proposes a general framework of best practices and processes to streamline reporting abuse of the domain name system (DNS).[5] The framework extends beyond abuse of the DNS to all Internet abuse, as abuse of the DNS is a subset of the overall abuse handling challenge. This effort is focused on determining approaches and methodologies that could ultimately reduce the severity and duration of victimization for end-users. This report focuses on one specific area of the DNS abuse lifecycle, namely abuse handling. Other topics in the space, including, but not limited to, prevention, mitigation methods, and education may be explored in future SSAC work.

This SSAC report was created by a work party that was formed of persons from varied backgrounds and relevant knowledge from both within the SSAC membership and invited guests[6] with specific interest and relevant expertise in DNS abuse detection and resolution. See Sections 10.1 and 10.2 for specifics.

This report also owes significantly to recent work attempting to apply the abstraction of "interoperability" from Internet protocol development and engineering to policy, particularly the notion of "legal interoperability" as developed by the Internet & Jurisdiction project.[7] There are several critical ideas that seem to apply. First, actors are partly or completely autonomous; in the network realm there's the expectation that network operators have control over their technology and infrastructure ("my network, my rules"), and in the policy realm those actors may be states, transnational entities such as ICANN, or service providers but the relevant attribute is that there's no authority with jurisdiction over all the relevant actors. Their interests are not identical and may be adversarial. Second, voluntary standards arise and are adhered to anyway where there's enough interest in lowering the cost of cooperation to solve a shared problem or meet a common need. Third, providing a neutral venue for developing such voluntary standards has proven extremely helpful or even necessary to reduce the costs of developing and implementing them.

[5] See Appendix A DNS Ecosystem

[6] See SSAC Operational Procedures, Section 2.8.6, https://www.icann.org/en/system/files/files/ssac-operational-procedures-v9.0-05jan20-en.pdf

[7] See Domains & Jurisdiction Program: Operational Approaches, Norms, Criteria, Mechanisms, https://www.internetjurisdiction.net/uploads/pdfs/Papers/Domains-Jurisdiction-Program-Operational-Approaches.pdf

There are already significant materials available on the general topics of detecting,[8,9,10,11,12,13] reporting,[14,15] and remediating DNS abuse,[16,17] and it is not the intention of this report to replace any such material that has been useful to the ICANN community and the larger Internet community. Instead, this report proposes an initial framework of and a way forward to reach shared descriptions and expectations of what mechanisms are used, by whom, and under what rules to coordinate activity against abuse by multiple involved parties. Ultimately, the SSAC would like to see this report as an input to ongoing community-wide efforts aimed to establish a universally accepted set of standards and practices that encompass the entire Internet ecosystem.

Defining abuse and other activities that should be acted upon by various parties is also not the intent of this report. Rather, this report focuses on where and how various activities should be reported and acted upon to most effectively and appropriately address abusive behaviors. Effective abuse mitigation in the DNS does not prevent all abuse on the Internet from occurring, nor does it necessarily suggest the DNS is the most effective or enduring place to accomplish mitigation. The purpose of this report is to specifically address forms of abuse that can at least be disrupted, if not mitigated, with the DNS, when it is appropriate to do so.

One major barrier for providers to take action against abusive activity is that service providers' ability to address abuse is limited to their Terms of Service (ToS), barring legal orders presented by authorities in a relevant jurisdiction. Requesting actions outside of those terms is asking a service provider to unilaterally break a contract with their customer. Terms of service for an operator allow the service provider to take actions to address abuse, but they are not a guarantee

[8] See M3AAWG Anti-Abuse Best Common Practices for Hosting and Cloud Service Providers, https://www.m3aawg.org/sites/default/files/document/M3AAWG_Hosting_Abuse_BCPs-2015-03.pdf

[9] See Janos Szurdi, Balazs Kocso, Gabor Cseh, Jonathan Spring, Mark Felegyhazi, and Chris Kanich. The long "taile" of typosquatting domain names. In *USENIX Security Symposium*, pages 191–206, 2014.

[10] See Manos Antonakakis, Roberto Perdisci, David Dagon, Wenke Lee, and Nick Feamster. Building a dynamic reputation system for dns. In *USENIX security symposium*, pages 273–290, 2010.

[11] See Daniel Plohmann, Khaled Yakdan, Michael Klatt, Johannes Bader, and Elmar Gerhards-Padilla. A comprehensive measurement study of domain generating malware. In *25th {USENIX} Security Symposium ({USENIX} Security 16)*, pages 263–278, 2016.

[12] See Daiping Liu, Zhou Li, Kun Du, Haining Wang, Baojun Liu, and Haixin Duan. 2017. Don't Let One Rotten Apple Spoil the Whole Barrel: Towards Automated Detection of Shadowed Domains. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS '17). Association for Computing Machinery, New York, NY, USA, 537–552. DOI: https://doi.org/10.1145/3133956.3134049

[13] See Ke Tian, Steve T. K. Jan, Hang Hu, Danfeng Yao, and Gang Wang. 2018. Needle in a Haystack: Tracking Down Elite Phishing Domains in the Wild. In Proceedings of the Internet Measurement Conference 2018 (IMC '18). Association for Computing Machinery, New York, NY, USA, 429–442. DOI: https://doi.org/10.1145/3278532.3278569

[14] See Guide to Registrar Abuse Reporting Practices, https://rrsg.org/wp-content/uploads/2020/03/Guide-to-Registrar-Abuse-Reporting-v1.8.pdf

[15] See Domain Abuse Activity Reporting, https://www.icann.org/octo-ssr/daar

[16] See Shuang Hao, Alex Kantchelian, Brad Miller, Vern Paxson, and Nick Feamster. Predator: proactive recognition and elimination of domain abuse at time-of-registration. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pages 1568–1579. ACM, 2016.

[17] See G. C. M. Moura, M. Müller, M. Davids, M. Wullink and C. Hesselman, "Domain names abuse and TLDs: From monetization towards mitigation," 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM), Lisbon, 2017, pp. 1077-1082, doi: 10.23919/INM.2017.7987441.

of action; there are still constraints on the service provider. Only where there is sufficient evidence to justify such an action, should an operator be expected to do so within the proper escalation path and timeframe. Thus, a provider's ToS are a key consideration for enabling effective anti-abuse outcomes.

Beyond having a sufficiently effective ToS in place, in order to effectively combat abuse and discourage repeat abusers, successful operators consistently apply the measures available in their ToS within set timeframes to significantly impact abusive activities. As with any business or organization, service providers each have internal competing interests and attitudes towards risk, and their organizational priorities change over time. Attention and resources dedicated to anti-abuse efforts thus vary between providers across the industry, and over time at single providers depending on their current priorities and approach to risk. This allows abusers to look for providers with lax enforcement of their ToS, and constantly test their ability to take advantage of all service providers.

Universal standards are critical to ensure that serial abusers do not intentionally seek out providers with lax terms or poor enforcement. For domain name registrations in generic top-level domains (gTLDs), ICANN has policies for dealing with specific abuses included in registries' contracts,[18] and country code top-level domain (ccTLD) regulators often provide specific rules for registries and registrars that reflect national laws or priorities.[19] Typically, such policies have focused on requirements for abuses that impact the Internet's infrastructure itself, or are considered to be serious criminal activities across all or most legal jurisdictions, such as the Council of Europe's Convention on Cybercrime.[20] This report does not opine on which abuse activities should be in service providers' contract terms.

The ICANN policy process is an appropriate tool for the greater ICANN community to set and encourage universal expectations for all ICANN contracted registries and registrars to adhere to when it comes to the types of abuses they should address. It is particularly suited for generating both policies and enforcement mechanisms for inclusion in legally binding contracts under specific jurisdictions. However, ICANN policy processes thus far have not provided a complete framework for combating all DNS abuse, nor can they as several key stakeholders in addressing DNS abuse are not subject to ICANN policy processes. Therefore, broadening the vista, the work of other bodies that have studied these issues thoroughly may set a baseline for universal abuse definitions, rather than creating an ICANN-unique set of definitions. Examples of such work include the Internet & Jurisdiction project,[21] the Budapest Convention on Cybercrime,[22] and the DNS abuse framework that many service providers have joined.[23] Together, ICANN's policy

[18] See ICANN Registry Agreement, https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-09jan14-en.htm

[19] See Terms and conditions for the right of use to a .dk domain name, https://www.dk-hostmaster.dk/en/terms

[20] See Details of Treaty No.185 Convention on Cybercrime, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

[21] See Internet & Jurisdiction Policy Network, https://www.internetjurisdiction.net/

[22] See Details of Treaty No.185 Convention on Cybercrime, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

[23] See DNS Abuse Framework, http://dnsabuseframework.org/

processes and other efforts within and beyond the ICANN community have served to establish both formal requirements such as those written into the ICANN gTLD contracts for registries and registrars, and less formal norms and policies that rely on broad acceptance and implementation for their enforcement.

1.1 Intended Audience and Use

This report is intended for use by audiences across both the Internet infrastructure and cybersecurity industries. This includes those entities that operate different aspects of the DNS as well as those entities that detect, report, and resolve DNS abuse, alone or as part of the wider ecosystem of technologies and actors enabling various types of victimization.

This report is neither designed to, nor is it intended to, propose any modification to existing ICANN contracts. It is intended as guidance for the above parties and the broader ICANN community to reduce the victimization of Internet users. This report's recommendation focuses on facilitating a broad community effort to determine mutual interest in setting community standards for the correct party for resolution, the reasonable time frame for resolution, and how interested parties might effectively document evidence for any reports made.

1.2 Outline for Report Content

The main areas of discussion in this report are the following:

- Definitions of Abuse
- Primary Point of Responsibility for Abuse Resolution
- Evidentiary Standards
- Escalation Paths
- Reasonable Timeframes for Action
- Availability and Quality of Contact Information

1.2.1 Definitions of Abuse (Section 2)

For the purposes of discussion, the effort relied on terminology definitions from the following sources, consistent with the Registry and Registrar Stakeholder Groups' recent adoption of these definitions:

A. DNS Abuse Framework[24]
B. Domains & Jurisdiction Program: Operational Approaches Norms, Criteria, Mechanisms[25]

The definitions cited here are widely discussed within the communities this report attempts to address. They are particularly focused on the DNS without being confined to the ICANN gTLD contracted parties or the ICANN community. To be clear there are additional abuses that are worthy of discussion. SSAC finds some of the specific definitions limited, and the above do not

[24] See DNS Abuse Framework, http://dnsabuseframework.org/

[25] See Domains & Jurisdiction Program: Operational Approaches, Norms, Criteria, Mechanisms, https://www.internetjurisdiction.net/uploads/pdfs/Papers/Domains-Jurisdiction-Program-Operational-Approaches.pdf

provide a general definition of abuse that may accommodate the evolving natures of abuse and cybercrime over time.

1.2.2 Primary Point of Responsibility for Abuse Resolution (Section 3)

Each incident of DNS abuse should have a reporting entry point (the party to whom you should report to first) in the DNS ecosystem where that abuse is resolved by policy and process. This allows for the creation of points-of-contact and escalation paths. More than one party may have a responsibility to deal with abuse of their product(s). For example, spam that promotes malware may be best addressed by the email platform or website operator, but there may be an additional role for the registrar or registry if, for example, a domain name was registered as part of the abusive activities. Identifying which party should be primarily engaged should be based on a clear hierarchy (see Section 5, Escalation Paths) that takes into account the effectiveness of the intervention, proximity to the issue, and the contractual complexity of relationships between the parties and the alleged abuser. In general, if a resource used for abuse was directly acquired by an abuser (purchased or provisioned), the corresponding service provider will be the most effective party to address the issue. Similarly, if a service was compromised, its owner and/or provider can play the primary role in remediating the compromise and thus the abuse.

1.2.3 Evidentiary Terminology and Standards (Section 4)

When service providers receive abuse complaints, they need evidence[26] supporting the complaint because from their perspective, all domain abuse is alleged until proven. The type, format, and detail of the evidence will likely vary by provider, geography, and jurisdiction. Evidentiary standards will ultimately be based on contractual terms, applicable law, and what is necessary for the service provider to enforce their terms of service and defend their actions. This does not, however, prevent the identification of common elements that may be considered an objective minimum evidentiary requirement for an abuse report across the industry. Setting objective standards of evidence to support action will enhance transparency and accountability for service providers. The wide adoption of such standards would provide for more efficient reporting and handling of abuse reports, reducing the time of victimization and effort needed for service providers to handle abuse reporting.

1.2.4 Escalation Paths (Section 5)

The creation of reasonable and transparent escalation paths is critical to quickly resolve abusive activity, perhaps especially with actors who are not part of the ICANN policy and contractual framework. Abuse may be handled differently based on business models or legal requirements. A complaint of abuse may need to move from the first point of contact to another point in the ecosystem that is involved in the provisioning or use of the domain (e.g., content delivery

[26] See Definition of Evidence, https://www.lexico.com/en/definition/evidence, Evidence: The available body of documented facts or information indicating whether a belief or proposition is true or valid.

networks (CDNs),[27] email providers (MX),[28] hosting) before an entity can effectively handle that report of abuse.

1.2.5 Reasonable Timeframes for Action (Section 6)

Motivating this report is a recognized need to have more rapid and predictable action in response to legitimate DNS abuse reports in the community. We also recognize the need to balance this aspiration with other factors, including economic, legal, and social. Each time frame discussed in this paper will depend upon the level of risk that a service provider is being asked to take. DNS service providers have a responsibility to seek some validation of the legitimacy of an abuse claim, but the service progression within the DNS may have a large chain of entities (hosting provider, registrar, registry, platform, Internet service provider (ISP)) who may have no relationship to one another. Having to engage with each provider independently to induce action can delay action and facilitate ongoing victimization. The DNS ecosystem needs to establish a balance.

1.2.6 Availability and Quality of Contact Information (Section 7)

A key dependency for the preceding items is to ensure that relevant and accurate contact data is readily available to assist in the rapid notification of suitable entities for the reporting of abuse. This should include methodology for obtaining contacts from the providers of the infrastructure through to the domain registrant.

2 Defining Some Aspects of the Problem and Existing Support Mechanisms and Resources

2.1 Defining DNS Abuse

The Framework to Address Abuse[29] and the Internet and Jurisdiction Policy Network's Operational Approaches, Norms, Criteria, Mechanisms[30] have definitions that serve as a basis for discussion in this report. These definitions state that DNS abuse is composed of five broad categories of harmful activity insofar as they intersect with the DNS: malware, botnets, phishing, pharming, and spam (when spam serves as a delivery mechanism for the other forms of DNS abuse). These two recent multi-stakeholder efforts provide the majority of text for the following definitions for each of these activities:

[27] A content delivery network is a system of distributed servers (network) that deliver pages and other web content to a user, based on the geographic locations of the user, the origin of the webpage, and the content delivery server. See Content Delivery Network (CDN) Meaning & Definition, https://www.webopedia.com/TERM/C/CDN.html

[28] A mail exchanger record (MX record) specifies the mail server responsible for accepting email messages on behalf of a domain name. It is a resource record in the DNS. It is possible to configure several MX records, typically pointing to an array of mail servers for load balancing and redundancy. See MX record, https://en.wikipedia.org/wiki/MX_record

[29] See DNS Abuse Framework, http://dnsabuseframework.org/

[30] See Domains & Jurisdiction Program: Operational Approaches, Norms, Criteria, Mechanisms, https://www.internetjurisdiction.net/uploads/pdfs/Papers/Domains-Jurisdiction-Program-Operational-Approaches.pdf

> **Malware** is malicious software, installed and/or executed on a device without the user's consent, which disrupts the device's operations, gathers sensitive information, and/or gains access to private computer systems. Malware includes viruses, spyware, ransomware, and other unwanted software.
>
> **Botnets** are collections of Internet-connected computers that have been infected with malware and can be commanded to perform activities under the control of a remote attacker.
>
> **Phishing** occurs when an attacker tricks a victim into revealing sensitive personal, corporate, or financial information (e.g., account numbers, login IDs, passwords), whether through sending fraudulent or 'look-alike' emails, or luring end-users to copycat websites. Some phishing campaigns aim to persuade the user to install malware.
>
> **Pharming** is the redirection of unknowing users to fraudulent sites or services, typically through DNS hijacking or poisoning. DNS hijacking can occur when attackers use malware to redirect victims to the perpetrator's site instead of the one initially requested. DNS poisoning causes a DNS server [or resolver] to respond with a false Internet Protocol (IP) address bearing malware. Phishing differs from pharming in that pharming involves modifying DNS entries, while phishing tricks users into entering personal information.
>
> **Spam** is unsolicited bulk email, where the recipient has not granted permission for the message to be sent, and where the message was sent as part of a larger collection of messages, all having substantively identical content.

These categories have been adopted within the ICANN realm in specific contracts, but do not represent all forms of DNS abuse that 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. Thus, no particular list of abuse types will ever be comprehensive. The Second Security, Stability, and Resiliency (SSR2) Review Team Final Report also observes this challenge in their Final Report and makes the following recommendation:[31]

> 10.2. Establish a staff-supported, cross-community working group (CCWG) to establish a process for evolving the definitions of prohibited DNS abuse, at least once every two years, on a predictable schedule (e.g., every other January), that will not take more than 30 business days to complete. This group should involve stakeholders from consumer protection, operational cybersecurity, academic or independent cybersecurity research, law enforcement, and e-commerce.

The SSAC supports the general concept of regular, community-driven review of DNS abuse definitions.

[31] See Second Security, Stability, and Resiliency (SSR2) Review Team Final Report, https://www.icann.org/en/system/files/files/ssr2-review-team-final-report-25jan21-en.pdf

There has not been consensus among all parties in the ICANN community to classify spam as DNS abuse as it is content-related and lacks both a uniform (world-wide) definition and any clear, homogeneous legal prohibition against specific use of mass email communications. However, a more strictly defined concept of spam (i.e., where spam is used as a delivery mechanism for one or more of the other four forms of stated DNS abuse) was included in both the recent Framework definition and by a Contracted Party House definition[32] of DNS abuse. In other words, as per the Framework's definition, generic unsolicited e-mail alone does not constitute DNS abuse, but it does constitute DNS abuse if that email is utilized in some form of fraud. However, other parties note that the definition of spam in the Contracted Parties' Framework is more narrow than the legal definitions of spam in many jurisdictions, including the European Union (EU),[33] the United States (US),[34] Canada,[35] Japan,[36] and Australia.[37] This highlights a challenge for service providers to accommodate conflicting laws across jurisdictions.

In general, while there are disparate views of abuse issues at the edges, service providers and reporters typically understand core abuse issues covered by these definitions and most providers have adopted Terms of Service conditions that allow them to address such core abuse types via actions such as account suspension, termination, or removal of abusive content. However, handling of abuse varies widely across the industry depending upon the practices of reporters and providers. This is a source of extended victimization as inefficiencies and delays are common due to lack of universal standards for reporting and acting upon different forms of abuse.

2.2 Website Content Abuse: Subjective approach

Registrars and registries are not required under their agreements with ICANN to monitor or suspend domain names based on website content abuse (abusive activities present on a website). The average abuse reporter attempting to stop a specific episode of abuse will tend to select the easiest and most available point of inquiry available to them. The actual selection of the initial escalation point, should, at its simplest, be attributed to the proximity of the escalation point to the abuse and the potential abuser. For example, a service provider may have specific legal obligations to deal in a more direct and effective manner (e.g., EU intermediary liability obligations),[38] or the abuse itself may be perpetrated by direct use of the infrastructure of such entities (e.g., hosting companies, email service providers, CDNs).

The line between free expression and illegal content varies across jurisdictions and cultures, and acceptable regional standards change over time. This has presented an ongoing challenge for

[32] See DNS Abuse Framework, http://dnsabuseframework.org/

[33] See Directive 2002/58/EC on Privacy and Electronic Communications: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52004DC0028

[34] See CAN-SPAM Act of 2003: https://en.wikipedia.org/wiki/CAN-SPAM_Act_of_2003

[35] See Canada's anti-spam legislation: https://www.fightspam.gc.ca/eic/site/030.nsf/eng/home

[36] See Act on Regulation of Transmission of Specified Electronic Mail

[37] See Spam Act 2003: https://en.wikipedia.org/wiki/Spam_Act_2003

[38] Where under applicable law (e.g. intermediary liability under the EU E-Commerce Directive 2000/31/EC, see https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32000L0031) where generally speaking certain service providers who have been given an actual notice of an ongoing issue may be required to intervene, lest they attract liability.

those in the DNS industry as there remains no universally accepted global standard for distinguishing between them. This results in a subjective review for reported abuse activities by every service provider. That being noted, many ICANN contracted parties do not see the minimum standard[39] as the goal, but as the starting point.

Unifying concepts of DNS abuse should be considered as a generally accepted goal, or minimum standard, with subjective and transparent efforts that expand upon that practice to be supported and encouraged. Abuse in the DNS does not solely fall on registry operators or registrars to remediate. Effective abuse mitigation must encompass the entire ecosystem, acknowledging that there remain a number of other providers in the DNS ecosystem who remain the more appropriate initial escalation point.

2.2.1 Disproportionality and Collateral Damage

Acting directly on a domain to address website content abuse, when the domain itself is not controlled by the abusive party, is usually a disproportionate remedy that can cause significant collateral damage and potentially have little to no lasting effect on the underlying abusive activity itself. A registry or registrar that receives a complaint about specific content cannot remove that content without disabling the entirety of the domain, including any third-level domains, other domains relying upon nameservers defined within the disabled domain, associated email hosting, and other content.

Disabling the resolution of a domain name is a serious remedy that may be appropriate in specific circumstances and is done routinely, at scale for many well documented and wide-ranging incidents or campaigns.[40] Disabling a domain name removes all content and associated services (e.g., email, authoritative DNS) for that domain and will impact any non-abusive behaviors as well as the identified abuse. However, a domain name registered recently (e.g., within 96 hours) is likely to cause less collateral damage if disabled because it is far less likely to be in widespread general use. Where the age of a domain is not a factor in the evaluation of abuse, a domain name registrant may not know that some portion of the DNS traffic associated with the otherwise benign domain is involved with anything abusive.

2.3 Defining Abuse Detection Roles

The abuse detection community is made up of a spectrum of entities from consumer to commercial. However, there are generally three roles.

> **Notifiers:** An authorized entity that has a special (contractual/legal) relationship with a service provider that has operational control over a domain name, hosting infrastructure, or other related Internet resources. The notifier has a privileged and often formal relationship with the service provider. A notifier identifies and reports a particular Internet resource for investigation/action (e.g., Internet Watch Foundation, National

[39] See DNS Abuse Framework, http://dnsabuseframework.org/

[40] Disabling a domain name does not necessarily disable content on a website, nor access to the website. This is a complex process with multiple possible scenarios with many possible technical details. Depending on how the website is configured, the content may or may not still be available. The website may still exist, and if a new domain is mapped to that website then the content will likely be available again using that new domain name.

Center for Missing and Exploited Children (NCMEC), a government law enforcement agency, or a national Computer Emergency Response Team (CERT)).

Reporters: An entity that reports potential abuse. A reporter's objective should be to report the alleged domain abuse requiring validation, following a standard of evidence and reporting path, related to the type of abuse. In the current Internet anti-abuse ecosystem, the bulk of reporters of abuse are organizations that exist to detect abuse, security vendors who offer mitigation services, or other organizations that exist to detect and report abuse.

Victims: A person or entity that is affected by an abuse issue or other transgression that has occurred. A victim can be a reporter, however, reporters are not usually the victim of the abuse. Entities that exist to report abuse by role and function will handle more abuse reports than any single victim or organization, and are often contracted to do so.

2.4 Impacts of Abuse

The impacts of cybercrime and other types of victimization on the Internet are felt by all, academic research and media coverage have created a high general awareness of many incidents, costs, and victims. Depending on methodology and data sources, estimates for direct victim losses range well into the billions of US dollars per year,[41] with overall impacts (time and expense due to lost commerce and remediation) ranging into the trillions per year.[42] This is not a new problem, but one that has been growing and evolving for over twenty years. What started as simple scams to steal access via dialup services such as AOL has morphed into sophisticated attacks of all varieties. Words like "phishing", "ransomware", and "botnets" have all been coined in that time and are now part of the common industry vernacular. The impacts on businesses, governments, critical infrastructure, individual privacy, and other aspects of our lives are felt by all and are considered a risk to most businesses and governments.

2.5 Abuse of Identifiers

Nearly all forms of abuse on the Internet require identifiers in order to occur, and very often this includes domain names. Interruption of the use of those identifiers, once discerned, is an important tool for limiting damage. The Internet is a decentralized system, with no central authority, and with operators agreeing via standards and arrangements on the exchange of data, connectivity, and issuance of necessary identifiers. These resources often can be exploited with or without their owner or user's consent via vulnerabilities, fraudulent sign-ups, compromised accounts, and inadequate security protections.

[41] See 2019 Internet Crime Report Released, https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120

[42] See Global Cybercrime Damages Predicted To Reach $6 Trillion Annually By 2021, https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

2.6 Preliminary Considerations & Appropriate Mitigation Paths

Once the identifiers are known, then a number of logical steps should be considered. The most appropriate next task is to consider who may be responsible for the identifier, or who is capable of interrupting the use of that identifier. There are methods to determine what entities control some Internet infrastructure, however, they are not consistently available, defined, or accurate. To further complicate the issue, once the correct entity (or entities) are determined, and the relevant identifiers discerned, one must then pursue the most appropriate means of mitigation. In doing so, one must take into account the impacts, not only on the abusive activity, but on other, non-connected users or services, or the service provider themselves, all of whom may be affected by the action taken.

The two primary mitigation methods for dealing with abuse issues are:

1) blocking or filtering communications between victims and the source of the abuse, and
2) notification and take-down requests of the abusive content itself.

Blocking and Filtering: Blocking and filtering can be quick to implement,[43] but do not solve the underlying issue, and are difficult to maintain at scale. Blacklists and lists of suspect DNS entities are often generated by algorithms that work at machine speed, and that can be deployed very quickly into an ISP's infrastructure or various perimeter security solutions.[44] These can be fraught with false positives and also may grow stale very quickly, and maintaining a very large list is beyond the capability of even the most advanced tools.[45,46,47] They also can lead to significant collateral effects if a resource blocked (e.g., domain name, IP address range, email servers) supports other non-abusive services.

Notification and Take-Down: Notification and take-down can lead to a cessation of the actual abuse (and resultant victimization), but may take a long time, have inconsistent outcomes, or impact other users of resources that are removed if they are applied too broadly.

Both mitigation methods come with legal complications, depending on the abuse claimed, the jurisdiction of the parties, or the impact (perceived or otherwise) of the fundamental freedoms of the Internet user.[48] The worldwide scale of hundreds of thousands of independent service

[43] Initial deployment of blocking/filtering technology and policies may vary depending upon chosen implementation(s), but ongoing updates to include newly reported activities are typically very fast.

[44] See Block newly-registered domains to reduce security threats in your organisation, https://www.tripwire.com/state-of-security/featured/block-newly-registered-domains-to-reduce-security-threats-in-your-organisation/

[45] See SAC050: DNS Blocking: Benefits Versus Harms – An Advisory from the Security and Stability Advisory Committee on Blocking of Top Level Domains at the Domain Name System, https://www.icann.org/en/system/files/files/sac-050-en.pdf

[46] See Jung, Jaeyeon, and Emil Sit. "An empirical study of spam traffic and the use of DNS black lists." Proceedings of the 4th ACM SIGCOMM conference on Internet measurement. 2004. https://dl.acm.org/doi/abs/10.1145/1028788.1028838

[47] See DNS Blocking: A Viable Strategy in Malware Defense, https://insights.sei.cmu.edu/sei_blog/2017/06/dns-blocking-a-viable-strategy-in-malware-defense.html

[48] See Report on the role of digital access providers, United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 30 March 2017, https://www.ohchr.org/en/issues/freedomopinion/pages/sr2017reporttohrc.aspx

providers, and millions of victims who are often serviced by thousands of vendors in the security space, the ecosystem for both blocking/filtering and abuse notification/response is large, diverse, and complex.

2.7 Effects on Service Providers

Abuse not only affects the victim, which of course remains the primary focus, but it also directly impacts the service providers in many ways. Service providers, for example, typically have an abuse reporting function that handles complaints of user behavior or compromised systems or accounts. There is very little standardization across single industries, much less the entire Internet ecosystem, on methods of processing and handling abuse reports and mitigations. With limited and inconsistent adoption of standardized reporting by incident responders, it can be a substantial cost to maintain this function. Service providers can also be impacted when there is abuse at scale in an area they may control. For example, a TLD or Autonomous System Number (ASN) may get blocked by significant portions of the Internet if abuse rates are high within that name or number space. Abuse at scale is a pervasive problem that erodes trust in the overall ecosystem.

2.8 Existing Support Mechanisms and Resources

There is no central authority, regulatory body, or industry organization that encompasses the entirety of this abuse/anti-abuse ecosystem. However, as many parties wish to streamline processes, improve accuracy, and increase effectiveness, several different cross-community efforts and organizations have sprung up to address different aspects of abuse. Some well-known examples with long histories include the Anti-Phishing Working Group (APWG)[49] which focuses on phishing, but also malware, botnets, and other e-crime; the Messaging, Malware, Mobile Anti-Abuse Working Group (M3AAWG)[50] which concentrates on spam, messaging abuse, and their supporting infrastructures; and the Forum of Incident Response Security Teams (FIRST)[51] that brings together CERTs[52] from around the world who work for both nation-states and industry. More recent efforts have sprung up that take on many of the cross-border and cross-sector challenges identified over the past decade. Examples of these newer groups include the Internet and Jurisdiction Policy Network[53] with an emphasis on cross-border harmonization of policy and process, the Cybersecurity Tech Accord[54] with an emphasis on the Internet of Things (IoT), the Public Interest Registry's DNS Abuse Institute[55] with a focus of abuse of the DNS system, and the Digital Trust and Safety Partnership[56] focused on consumer safety and trust in online content. Many other efforts exist as well, and usually involve not just incident responders, but some portion of the service provider industries.

[49] See APWG: Research, https://apwg.org/research/

[50] See Why M3AAWG? https://www.m3aawg.org/about-m3aawg

[51] See FIRST Vision and Mission Statement, https://www.first.org/about/mission

[52] See Computer emergency response team, https://en.wikipedia.org/wiki/Computer_emergency_response_team

[53] See Internet and Jurisdiction Policy Network, https://www.internetjurisdiction.net/

[54] See Cybersecurity Tech Accord, https://cybertechaccord.org/

[55] See PIR Launches New Institute to Combat DNS Abuse, 17 February 2021, https://thenew.org/pir-launches-new-institute-to-combat-dns-abuse/

[56] See Digital Trust & Safety Partnership, https://dtspartnership.org/

These types of groups have developed some standards for reporting, blocking, and other security responses along with associated communications protocols, but none have managed to establish a universally accepted set of standards that encompass the entire Internet ecosystem. Reach seems to be a major challenge in such efforts, as these groups have typically formed either to take on specific issues (e.g. phishing, spam, or malware) or formed within specific industry or interest areas (e.g. incident response, data sharing). Despite over twenty years of efforts in this space with some significant improvements, consistent, timely, and accurate mitigation of abuse across the Internet, including DNS abuse, remains an elusive goal.

2.8.1 Notifier and Reporter Formalized Programs

To combat DNS abuse more effectively, the concept of a "notifier program" has been created and utilized by various entities in the ecosystem and by several prominent law enforcement agencies (e.g., Federal Bureau of Investigation (US) and the United Kingdom National Crime Agency), independent organizations (e.g., Legitscript,[57] NCMEC[58]), and service providers themselves (e.g., Freenom[59]). Similarly, some ccTLD operators and ISPs have such reporting and action agreements with their national CERT team. Such programs aim to expedite DNS abuse remediation by requiring parties to trust reporters that have clearly substantiated evidence of abuse, and whose requested action can be taken without fear of false-positives and or loss of indemnification. This concept requires an explicit network of trust between all parties along with reporting protocols and processes all participants adhere to. These attributes address many of the challenges in this space and provide informative examples for improved abuse handling. However, there are challenges in scaling these programs so that all participants may reap their benefits. First, the semi-closed nature of notifier programs makes scaling the programs difficult. Second, each program develops its own standard and processes independent of other programs. Agreement amongst such groups or more broadly, across the ecosystem, on standards, practices, protocols, etc. would likely make such efforts more effective and accessible.

Even though no organizations exist for the standardization of DNS abuse, the APWG has been using an accreditation process for participation in their data submission program. The program uses a “formal mechanism for an enterprise to be accredited by the APWG to send reports to the APWG URL Blocklist (UBL) directly and, further, to assign those reports a confidence factor commensurate with the expertise and authority of the reporter.”[60] Once qualified, organizations can use their credentials to submit bulk reports for processing, reducing the time of delivery to the UBL as well as accelerating processing and clearance of reports through the UBL to end-users. This accreditation process illustrates the benefits of an approach that utilizes an independent facilitation body verifying community-defined standards to minimize response time.

[57] See Registrars and Registries, https://www.legitscript.com/industry/registrars/

[58] See 18 U.S.C. § 2258c

[59] See Anti Abuse API, https://www.freenom.com/en/antiabuse_api.html

[60] See APWG Accredited Reporter Data Submission Program, https://docs.apwg.org//reports/Accredited_Reporter_Intro_and_Application.pdf

A similar independent program could be established for the purpose of notifying ICANN contracted parties and other infrastructure entities.[61] Such a program could be based on the procedures, timing, evidentiary standards, burden of proof, and other processes outlined in this report, and developed further by an independent, industry-wide facilitator to ensure participation and harmonization among the Internet-wide stakeholder community. Consequently, such a program may lend itself well to addressing the DNS abuse issues in a more streamlined and efficient manner without sacrificing the benefits of standardization within their purview, namely, reducing the timeframe of abusive activities and the costs for service providers to handle abuse queues. However, on their own, notifier programs are not a panacea for handling abuse in the DNS.

3 Primary Point of Responsibility for Abuse Resolution

The primary consideration of a starting point for abuse issues of any type is understanding what service or services were used to perform the abuse. Does it involve the creation of web content, identifiers, platform accounts, traffic, or messages? Was a service compromised in order to perpetuate the abuse, the compromise being an abuse itself? Answers to these questions are required by anyone who wants to effectively report and mitigate abusive activities of all types and create the proper requests for mitigation. The understanding that all reporters may not be able to answer all of these questions comprehensively is addressed further in Section 4.

The most effective and proportional solution to a particular abuse problem requires understanding the nature of the enabling infrastructure and dealing directly with those providers in the appropriate manner. Appendix B provides a suggested starting point for various configurations of infrastructure utilized for abusive activities. In general, if a resource used for abuse was directly acquired by an abuser (purchased or provisioned), the service provider who provided that service will be the most effective party to address the issue. Similarly, if a service was compromised, the legitimate user of that service and/or the provider of the compromised service will play the primary role in remediating the compromise, and thus the abuse.

DNS abuses are enumerated for gTLD operators in Specification 11 (3)(b) of ICANN's model contract for registries:[62]

- pharming,
- phishing,
- malware,
- botnets, and
- other types of security threats

[61] A pilot program of this nature was recently launched by the US National Telecommunications and Information Association (NTIA), Food and Drug Administration (FDA) and several gTLD registries. See https://www.commerce.gov/news/press-releases/2020/06/commerce-department-announces-ntia-pilot-program-hhs-fda-fight-illegal

[62] See Advisory, New gTLD Registry Agreement Specification 11 (3)(b), https://www.icann.org/resources/pages/advisory-registry-agreement-spec-11-3b-2017-06-08-en

The primary point of responsibility for the management (including abuse management) of a TLD lies with the registry operator. The primary responsibility for escalation and remediation of DNS abuse of an individual domain name lies with the registrar holding the contract with the registrant. Barring urgent circumstances (e.g., the severity of imminent harm), the registrar should be the first to take action against an abusive domain. When a registrar declines to act or is nonresponsive, the registry would then be in a better position to take direct action. However, while registries have often performed such actions, in general registries do not have any contractual relationship with a registrant that would otherwise give them the ability to act against terms of service or acceptable usage policy which may present legal, financial, and reputational risk for registries.

The registry operator may receive the initial reports of abuse, but ordinarily, escalate to the registrar on record. If for example, the domain name reported for a phishing attack is one that has been compromised and the URL points to new content, the registrar on record, or even the registrant in the case of a compromised domain, may be the party who can take the most immediate and effective action. The hosting company may also be the most relevant and effective party to respond to the reported abusive content. Challenges remain in the identification of that hosting company or CDN, which may make escalation difficult (e.g., the CDN can mask the technical details of who is hosting a domain and how it is configured requiring additional steps).

The availability of readily accessible contact information becomes increasingly difficult the further the responsible party for the abuse is downstream from the registry. Without information available from the registrar, some of the paths to contacting a potentially responsible party are limited, or non-existent, for a multitude of reasons. Thus, the primary point of contact (not necessarily for action) for DNS abuse will often be the registrar. The registrar has the most non-public information available to contact registrants. It is for this reason that a primary means for concerted action to address abuse should be for the registries, registrars, hosting companies, CDNs, and other players to share information with each other.

4 Evidentiary Terminology and Standards

Evidence is the available body of facts or information indicating whether a belief or proposition is true or valid. The four types of evidence generally recognized by courts include demonstrative, real, testimonial, and documentary. For the context of this report, the use of the term evidence refers to *demonstrative* and *documentary*.

A party with a report regarding abuse domain(s) has the responsibility of providing evidence and documentation. The amount of documentation regarding the abuse required varies from provider to provider, case to case, and type to type. The evidentiary standards should require documentation of the elements of the abuse and, in some complex cases, a demonstration of how the abuse is occurring.

4.1 Collection of Grounding Evidence

Each type of abuse has different types of evidence or proof of transgression available to qualify the specific abuse that happened on a particular domain. In many cases, the evidence can be

captured in a visual context. One of the particular challenges to gathering evidence of domain abuse is its temporal nature. The domain may only be used for a short time in the perpetration of fraud (e.g., phishing), creating the challenge of capturing the evidence in a narrow time window. During this time, visual evidence (web site screenshot) may also be captured if it exists. Mail server fraud may be evidenced by MX records and/or email headers. Other abuses such as botnets and malware downloaders (such as ransomware) may only be evidenced by recording behavior on the victim's computer system.

The SSAC recognizes that what constitutes evidence may vary among service providers, geographies, and jurisdictions, adding an extra layer of complexity to the process of providing evidence of DNS abuse. It is also important to note that a wide variety of actors can be notifiers, and designating them as such is largely, although not completely,[63] at the discretion of receiving entities. The receiving entity has to weigh the risks of accepting a notifier's report as actionable, without any further verification, against the risk of acting on the unsubstantiated evidence presented. The lack of standard reporting methods and channels, along with varied levels of report quality, create a difficult support problem for service providers receiving claims of abuse.

As discussed above, the collection of evidence has a temporal nature. The better the evidence collected during the abusive transgression, the more likely a responsible party will feel comfortable intervening. Evidence collected after the abuse has occurred is less compelling, though still may be sufficient.

Collection of evidence should include several factors that help demonstrate a specific abuse has occurred, and what type of abuse it is:

- **Temporal Relevance:** When did it happen? How long after the registration did the abuse occur? How long after the abuse was detected did the evidence get logged or captured? All timestamps must include full dates and time zones of the observations to demonstrate accuracy.

- **Visual:** Was there an "A" or "AAAA" DNS record logged for the domain?[64] These are fundamental for assuring network access to the domain. Was there content hosted on the domain that was not a parked page[65] record and that was captured via screenshot or other means?

[63] For example, a party may have a legal obligation in their jurisdiction to act, without discretion, on the report of a particular notifier (e.g., applicable Court order, valid warrant (in jurisdiction) etc.

[64] An A record maps a domain name of the IPv4 address of the computer hosting the domain. An A record is used to find the IP address of a computer connected to the internet from a name. An AAAA record serves similar functionality, but for IPv6 addresses.

[65] A parked domain is a registered domain name that is active but is not associated with a specific website. Instead, a parked domain displays a parked page to users who visit the URL. A typical parked page has a simple layout with a list of links related to the domain name. These links typically generate advertising revenue for the parked domain's owner when users click on them.

- **Behavioral:** Logs of activities regarding the domain name itself, such as records in the zone, changes in delegations and or the whois record, including passive DNS?[66]

- **Demonstration:** Can the reporter demonstrate, with appropriately reliable evidence, the abuse for which the domain was used? Can the reporter make the case that this use violated the Terms of Service of the infrastructure responsible party in a fashion that supports rapid action against the abusive domain? This typically includes an explanation of the type of abuse, its impact, and its correlation to the anti-abuse policies of the responsible party.

5 Escalation Paths

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

Evidence of both the infraction or abuse and the amount of time that has passed from the initial reporting of the abuse can be reported to the next party in the escalation path. This type of standardization will allow for the eventual automation of steps in the abuse mitigation process.

6 Reasonable Time Frames for Action

The timely mitigation of DNS abuse is extremely important to minimize victimization of the abuse. As in the case of a phishing domain, the longer the domain resolves in the DNS (e.g., returning A, AAAA and/or MX records) the more potential victims of the phish. Understanding that there are different types of abuse is important to the assessment of how much time is reasonable to react to, and act upon, a domain involved in abuse. Domain abuse is designed to harm or defraud a consumer or end-user of the DNS, from stolen personally identifiable information (PII), or credit card fraud, to delivery of malicious code to the end-user's computer where it may become part of a botnet or be locked and encrypted for a ransomware fraud.[67] Thus, it is in the best interest of both the end-users and the infrastructure service providers to resolve the abuse as expeditiously as possible.

Providers who consistently ignore or take inordinate amounts of time without reasonable cause to respond to well-documented requests for action are a problem within the industry. There are ongoing efforts to track and identify such providers by various parties, but these efforts require broader industry-wide accepted methodologies and reporting. Creating a neutral clearing house for provider response behavior information may lead to the establishment of baseline behaviors that could institute industry norms for reporting and response.

[66] See Passive DNS - Common Output Format, https://tools.ietf.org/id/draft-dulaunoy-dnsop-passive-dns-cof-04.html

[67] Ransomware is a type of malware designed to block access to a computer system until a ransom is paid, often in the form of a cryptocurrency or financial transfer.

6.1 Escalations

One of the standards used by many operators that have abuse handling functions is to send notice to a party of an abuse that needs to be resolved and allow 24 hours for resolution of that abuse. This is guided primarily by contractual obligations that exist between said parties (e.g. registry relaying an abuse domain to a registrar) or practical experience in handling large-scale abuse queues. Some incidents may see shorter or longer intervals for re-notification or escalation depending upon the nature of the abuse. The escalation path for an incident is frequently reported first to a registry, who then reports it to the registrar, who then may report it to the registrar reseller, and finally, the report is presented to the registrant for action. This is a reporting chain of potentially 24-hour periods that could stretch as long as 96 hours before the abuse is addressed. Given the preceding model, a reasonable timeframe of 48 hours beyond the initial report would be optimum in reducing ongoing victimization from the domain. As the chain of entities may include 4-6 points of contact, a maximum time for escalation and remediation should be no longer than 96 hours.[68] Reasonable efforts should be taken to reduce this window to less than 96 hours.[69] There are multiple opportunities to automate these processes in a meaningful way that could reduce the total duration significantly, while still respecting expectations of due process.

6.2 Expedited Escalations

Where reports indicate an instance of abuse of heightened scale and severity, operators should aim to ensure that any such matters are remediated within an expedited time frame. The reasonable expectations for escalation and remediation of such should be commensurate with the potential harm threatened. For example, cases of domain names which have been connected to child sexual abuse and exploitation, or self-replicating malware should be remediated with great urgency.

7 Availability and Quality of Contact Information

A significant issue in abuse notifications to DNS ecosystem entities is the availability of, and access to, high quality contact information for the entities involved and who are best situated to take action. As the number of registries account for the smallest numbers of entities in the ecosystem and the relatively simple connection of a TLD to the registry operator, the registry operator is a logical first entry point in the chain. The TLD is tied to the registry operator, so a victim or other reporter has both easy access to operator information through IANA[70] and, from there, to the operator's website where the abuse contact can be located.[71]

The registry does not usually have a direct relationship with the registrant and may be unable to provide registrant contact information. The registry can provide a referral to the registrar of the

[68] 24 hours per party in the fully expanded escalation path. i.e., Registry - Registrar - Reseller - Hosting Provider (24x4=96hrs)

[69] These timeframes are suggested based on a limited review of industry practices in this work party.

[70] See for example registry information for .aaa TLD, https://www.iana.org/domains/root/db/aaa.html

[71] See Root Zone Database, https://www.iana.org/domains/root/db

domain, which in turn has the desired contact data. If query rate-limiting is in effect,[72] access to the registrar of record for a domain is not always available. The identity and designated abuse contact information of the registrar, as well as the designated name servers, should be generally and openly available. However, privacy protocols implemented after the General Data Protection Regulation (GDPR) went into effect,[73] privacy protection services, and aggregation of content on large platforms, make it difficult to determine the appropriate contact information when a registrant is the appropriate first contact.

The potential points of contact (listed in no particular order) for an abuse notification are:

1. Registry
2. Registrar
3. Registrar Resellers
4. Registrant
5. Hosting Provider
6. Content Delivery Network
7. Mail Provider
8. Internet Service Provider

Uncertainty in the current environment regarding responses to abuse reporting incentivizes reporting parties to use a 'scattergun approach',[74] (i.e., sending reports to all potential parties in the DNS ecosystem at the same time in the hope that one of them will react and address the abuse). While this approach can reduce response times, it comes at a cost. Namely, the wrong parties sometimes get notice and learn to ignore subsequent requests and notifications; the reporting party does not get a feedback loop wherein they learn what the appropriate party was; and a party may investigate the abuse only to find that another party has already reacted to the notification, thereby wasting time and effort. Each incident may vary, and notifying two or more parties initially or in sequence may be warranted depending upon the configuration of the abuse. Experience and playbooks help immensely in understanding how to handle various configurations of abusive activities.

Without a set of universal standards for service providers to implement for reporting abuse issues, reporting and resolving abuse becomes challenging for reporters. A reporter has to determine how, where, and when they can submit abuse reports to each individual service provider they may have to deal with. Thus, each report may become a custom exercise if they wish to have it dealt with expeditiously. Reporters may not expect a specific response or action, thus incentivizing over-reporting as an attempt to ensure a response from at least one provider. This affects all parties negatively, introducing costs to all, and increases overall victimization. If industry-wide standards were adopted by service providers for reporting requirements that

[72] See SAC101v2: SSAC Advisory Regarding Access to Domain Name Registration Data, https://www.icann.org/en/system/files/files/sac-101-v2-en.pdf

[73] The General Data Protection Regulation 2016/679 is a regulation in EU law on data protection and privacy in the European Union and the European Economic Area. It also addresses the transfer of personal data outside the EU and EEA areas.

[74] Scattergun refers to a way of doing or dealing with something by considering many different possibilities in a way that is not well organized.

included methods and response times aligned with reporters' capabilities, these problems would be largely mitigated. Other specific challenges may remain, including compatible hours of service and linguistic and translation issues, but are not systemic. However, getting all relevant stakeholders on the same page remains difficult.

There is an opportunity to create a single point of contact determination whereby a reporter can identify the type of abuse and get directed to appropriate parties. This can additionally lead to the appropriate escalation paths and the terms of service language necessary to have that type of abuse addressed. This works within both the reporter and notifier models, while acknowledging that knowing where to report the abuse is paramount to abuse resolution. By creating a common framework of reporting and escalation mechanism for abuses, the scaling challenges of many reporters to many service providers is restructured into a standardized model that will better coordinate and address abuse reports. Creation, maintenance, and dissemination of this framework throughout the ecosystem will require ongoing effort and likely a common facilitator to be successful.

8 Findings

In this report the SSAC has outlined opportunities to address DNS abuse through the implementation and introduction of standardized best practices. All are, in the opinion of the SSAC, achievable objectives.

Lack of coordination leads to inconsistent approaches to DNS abuse management
Acknowledging the topics as highlighted and discussed in this report, the SSAC notes a lack of consistency in the approach and coordination of DNS abuse management. This is caused by a lack of universal protocols, standards, and best practices in the areas highlighted in this report. This is further exacerbated by a dearth of entities acting to convene relevant stakeholders, or coordinate and facilitate tasks necessary for mitigating DNS abuse, including but not limited to, identification, evidentiary standards, escalation pathways, and the means for remediation. While many separate entities exist that may perform a similar function in subsections of this problem space, there remains no single entity that can cover the breadth of the topics discussed. To be clear, this does not mean that the issues identified require, or would benefit from, a mandatory centralized solution, either legally or operationally. However, in some cases, a shared interest and framework will make it more logical to appoint a Common Abuse Response Facilitator.

The SSAC observes there is a general desire in the ICANN community to begin taking organized action related to DNS abuse. Most recently, the SSR2 Review Team recommended in their Final Report,[75]

> 13.1. ICANN org should establish and maintain a central DNS abuse complaint portal that automatically directs all abuse reports to relevant parties. The system would purely act as an inflow, with ICANN org collecting and processing only summary and metadata, including timestamps and types of complaint (categorical). Use of the system should become mandatory for all generic top-level domains (gTLDs); the participation of each

[75] See Second Security, Stability, and Resiliency (SSR2) Review Team Final Report, https://www.icann.org/en/system/files/files/ssr2-review-team-final-report-25jan21-en.pdf

> country code top-level domain (ccTLD) would be voluntary. In addition, ICANN org should share abuse reports (e.g., via email) with all ccTLDs.

While the SSAC declines to opine on this specific recommendation in this report, we note the Review Team's call for a centralized entity responsible for coordinated action.

Common Abuse Response Facilitator

The SSAC believes that an opportunity exists for the creation of a single entity to independently convene, facilitate, guide, and provide clarity and predictability to all stakeholders in the greater DNS ecosystem. These stakeholders would include Internet users as well as the industry providers and those who perform specific functions for the industry. Different players can retain their autonomy, but acknowledge shared problems and interests, while creating protocols and procedures for cooperation. This is an underlying architectural principle in the Internet, including the DNS service, and has also been cited in the work of the Internet & Jurisdiction Project.[76] This observation is an important distinguishing factor for the proposed role of the Common Abuse Response Facilitator. The Common Abuse Response Facilitator, then, should be promoting the development of shared protocols and best practices for players to interact. They may also fulfill the role of educating all those involved and therefore supporting the practical applications of those protocols and best practices as identified.

The role of the Common Abuse Response Facilitator would be to develop and implement a functional Internet-wide community model to directly confront the problem of Internet abuse, including DNS abuse. Although ICANN plays a role in the enforcement of the limited aspects of the contracts of both registries and registrars via their compliance function, they are restricted in this sphere because ICANN's contractual function does not encompass some of the broader DNS ecosystem entities (e.g., hosting providers, ISPs, and CDNs). However, the ICANN community is in a position to play a key role to support the development and creation of this entity. The proposed entity should ideally be a wholly independent non-governmental, not-for-profit organization that can act as a facilitator for the entire DNS ecosystem, where the DNS ecosystem includes ICANN contracted parties and other entities key to both the functionality of, and resolution of abuse in, the DNS. ICANN has played similar roles in other initiatives that overlap with its mission and remit but extend into the wider Internet ecosystem. Such efforts include ICANN's support for and participation in the Universal Acceptance Steering Group[77] as well as the series of ICANN DNS Symposiums bringing together all parties with interest in the health, stability, and security of the DNS.

The SSAC proposes that the mission of a Common Abuse Response Facilitator should include:

A. A practical scoping of the problem space within which the designated entity will operate.
B. A convening of relevant stakeholders in order to determine the scope and impact of the problem space that needs resolution or may need future consideration.
C. A process for determining and implementing a "best practices model" for the different entities in the ecosystem for mapping and resolving abuse.

[76] See Domains & Jurisdiction Program: Operational Approaches, Norms, Criteria, Mechanisms, https://www.internetjurisdiction.net/uploads/pdfs/Papers/Domains-Jurisdiction-Program-Operational-Approaches.pdf

[77] See Universal Acceptance, https://uasg.tech/

D. A process for creating or determining an evidentiary standard among the stakeholders for all types of abuse that require mitigative action within the DNS ecosystem.
E. Development and execution of a common framework, using SAC115 as a proposed starting point, for reporters and notifiers of domain abuse activities.
F. An abuse reporting approach that includes the following elements:
    a. The primary point of responsibility for abuse resolution;
    b. evidentiary standards;
    c. escalation paths;
    d. reasonable timeframes for action;
    e. availability and quality of contact information;
    f. repository for anti-abuse best practices for the DNS ecosystem; and
    g. a forum for further development of the above.
G. Establishment of standardized methodologies and definitions to encourage confidence and trust in reports and, where an operator deems appropriate, in specific reporters. In this sense, the framework may aid in the streamlining and facilitation of "notifier" programs.
H. Periodic reporting to educate and inform on the effectiveness of the Common Abuse Response Facilitator's programs. (e.g., adoption of the model, numbers of requests for information and any measurements of success).

9 Recommendations

While the SSAC acknowledges the opportunity and need to create the anti-abuse efforts outlined in this report, it is not advocating for any particular organization or entity to fulfill them. The SSAC does anticipate, however, that ICANN org and the ICANN community will continue to fulfill their role to encourage unified community-led efforts. To that end, we make the following 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.

This community effort should include domain registration providers that are part of the ICANN community. In addition, it should seek participation and input from communities beyond the ICANN community, such as DNS infrastructure providers, content hosting providers, and the incident response community, and anti-abuse community. Other organizations that have worked on Internet abuse should also be invited.

10 Acknowledgments, Statements of Interest, and Dissents, Alternative Views and Withdrawals

In the interest of transparency, these sections provide the reader with information about aspects of the SSAC process. The Acknowledgments section lists the SSAC members, outside experts, and ICANN staff who co-authored or contributed directly to this particular document

(Contributors) or who provided reviews (Reviewers). The Statements of Interest section points to the biographies of all SSAC members and invited guests, which disclose any interests that might represent a conflict—real, apparent, or potential—with a member's or invited guest's participation in the preparation of this Report. SSAC members act as individuals, not as representatives of their respective organizations. The Dissents and Alternative Views sections provide a place for individuals to describe any disagreement with, or alternative view of, the content of this document or the process for preparing it. The Withdrawals section identifies individuals who have recused themselves from the discussion of the topic with which this Report is concerned. Except for members listed in the Dissents and Alternative Views or Withdrawals sections, this document has the consensus approval of all of the members of SSAC.

10.1 Acknowledgements

The committee wishes to thank the following SSAC members and invited guests for their time, contributions, and review in producing this report.

SSAC Members
Jeff Bedser (Work Party Chair)

Contributors:
Tim April (contributor)
Ben Butler (reviewer)
Lyman Chapin (reviewer)
Steve Crocker (reviewer)
Patrik Fältström (reviewer)
James Galvin (contributor)
Robert Guerra (reviewer)
Julie Hammer (contributor)
Merike Kaeo (contributor)
Warren Kumari (reviewer)
KC Claffy (reviewer)
Danny McPherson (contributor)
Ram Mohan (reviewer)
Rod Rasmussen (contributor)
Mark Seiden (reviewer)
Doron Shikmoni (contributor)
Matthew Thomas (reviewer)
Suzanne Woolf (contributor)

Invited Guests
Kristine Dorraine (contributor)
Chris Lewis-Evans (contributor)
Alan Woods (contributor)

ICANN Staff
Danielle Rutherford (editor)
Andrew McConachie

Kathy Schnitt
Steve Sheng
Patrick Jones

10.2 Statements of Interest

SSAC member biographical information and Statements of Interest are available at: https://www.icann.org/resources/pages/ssac-biographies-2021-01-07-en

Invited Guests' Statement of Interest are available at:
https://community.icann.org/display/gnsosoi/Kristine+Dorrain+SOI
https://community.icann.org/display/gnsosoi/Chris+Lewis-Evans++SOI
https://community.icann.org/display/gnsosoi/Alan+Woods+SOI

10.3 Dissents and Alternative Views

10.3.1 Rationale

We (the SSAC members named in Section 10.3.7) agree that improved processes to streamline reporting DNS abuse and abuse on the Internet are much needed, and that popularizing better practices could be very helpful. However, we have doubts about whether a "Common Abuse Response Facilitator" can be a truly impactful endeavor. We also dissent from some statements made in this Report, as specifically noted below.

Unfortunately the Report has not focused on what ICANN can do within its remit to combat abuse, and instead suggests addressing the entire Internet ecosystem and all of its various kinds of providers, all of which occupy different sectors with different technical responsibilities and economic models. This ambition reduces the chances of success. There are options for doing impactful work within ICANN's remit, including the creation of effective and uniform solutions that can be incorporated in ICANN's contracts with its registrars and registry operators.

10.3.2 Alternative View: The "Common Abuse Response Facilitator" Concept

It is unclear how the proposed "Common Facilitator" can move the needle on abuse, and further discussion of the idea should include an assessment of the idea's chances for success. At best, we believe that the "Common Abuse Response Facilitator" may provide some incremental gains, by raising awareness and by popularizing voluntary standards and techniques that some providers may decide to adopt. At worst, the "Common Facilitator" project may expend money and time for little return, or no return that can be measured. The endeavor may give the appearance that ICANN and other communities are "doing something about abuse," but ICANN and other stakeholders should be focused on measurable effectiveness.

As this Report notes, decentralized decision-making, a lack of oversight in most sectors, and market forces are features of the Internet. These are things that a "Common Facilitator" would have no ability to affect, and the Report does not offer strategies for doing so.

A main dilemma in this space is economic interest. Generally, every provider of Internet resources decides what is best for itself, and cannot be compelled to behave differently.[78] Each provider decides how much money it wants to spend on anti-abuse work, how much it wants to know about its customers and what they are doing, and how proactive or reactive it wants to be in its anti-abuse work. Internet service companies in every sector have decided to handle their abuse reporting and mitigation processes in certain ways that they believe are appropriate for their businesses. This includes the Internet's largest companies, which have great resources available to them, know what alternatives are available to them. Companies large and small in the domain name industry are also aware of the options available to them, and they have made their choices too. Will companies like these depart from their business interests and corporate philosophies and alter their practices because a "Common Facilitator" suggests they do, and creates some other best practices?

Providers of Internet resources do currently have some best practices in their sectors that they can follow.[79] Various anti-abuse best practices have been explored at ICANN over the years.[80,81,82] There is much information to help providers identify abuse on assets they have visibility on or control. There has been reporting to the correct providers for many years, by professional parties who know where to report and how to report with suitable evidence. But still the abuse problems remain as great as ever, and some large and experienced providers do not respond effectively to well-supported abuse reports. It appears that a lack of best practices and good reporting may not be the biggest problems that need solving.

10.3.3 Dissent: Response Times

Section 6.1 ("Escalations") states:

> One of the standards used by many operators that have abuse handling functions is to send notice to a party of an abuse that needs to be resolved and allow 24 hours for resolution of that abuse. This is guided primarily by contractual obligations that exist between said parties (e.g. registry relaying an abuse domain to a registrar) or practical experience in handling large-scale abuse queues . . . Given the preceding model, a reasonable timeframe of 48 hours beyond the initial report would be optimum in reducing ongoing victimization from the domain. As the chain of entities may include 4-6 points of

[78] Except of course by the laws of or regulators within their jurisdiction. ICANN is a perhaps singular exception, having some contractual authority over companies in a particular space. But otherwise no entity has control over any sector of Internet services, such as hosting, apps, the IP space, routing, etc.

[79] For example: M3AAWG's best practices series for mail senders and anti-abuses operations (see: https://www.m3aawg.org/published-documents); NIST's frameworks for cybersecurity, computer security, and risk management (see: https://www.nist.gov/cybersecurity); ISO standards; best current practices for the assignment and use of IP addresses promulgated by RIRs; etc.

[80] "Discussion Paper on the Creation of non-binding Best Practices to help Registrars and Registries address the Abusive Registrations of Domain Names." ICANN GNSO, 2011. https://gnso.icann.org/sites/default/files/filefield_26745/discussion-paper-rap-best-practices-28sep11-en.pdf

[81] "Registration Abuse Policies Working Group Final Report." ICANN GNSO, 29 May 2010. https://gnso.icann.org/sites/default/files/filefield_12530/rap-wg-final-report-29may10-en.pdf

[82] "Competition, Consumer Trust, and Consumer Choice Review Final Report." ICANN review team, 8 September 2018. https://www.icann.org/en/system/files/files/cct-final-08sep18-en.pdf

> contact, a maximum time for escalation and remediation should be no longer than 96 hours.

We do not know where this timeline came from, it is unsupported by any references, and we do not believe it is advisable. In reality, the window for effective action is much, much shorter, and if the above is followed, it will lead to unnecessarily slower and less effective anti-abuse efforts. The suggested time frames in section 6.1 contradict security research and the practical experience of security responders. For example, phishing studies confirm that the window for effective action is a few hours.[83] Similarly, many domains used for distributing malware, or for botnet command and control, are only active for 24 hours. Thus, it is more sensible to tailor response times to the threat, rather than set an arbitrary, one-size-fits-all limit. The suggested timeframes also assume that simultaneous notification to multiple points of contact will not be the norm. Response times of 48 to 96 hours can allow great harm to take place, and if such timeframes are promoted as "reasonable," the public will be ill-served.

10.3.4 Dissent: Action by Registry Operators

Section 3 states:

> The primary responsibility for escalation and remediation of DNS abuse of an individual domain name lies with the registrar holding the contract with the registrant. Barring urgent circumstances (e.g., the severity of imminent harm), the registrar should be the first to take action against an abusive domain. When a registrar declines to act or is nonresponsive, the registry would then be in a better position to take direct action. However, while registries have often performed such actions, in general registries do not have any contractual relationship with a registrant that would otherwise give them the ability to act against terms of service or acceptable usage policy which may present legal, financial, and reputational risk for registries.

We disagree with this statement because it is overly simplistic and is not consistent with established best practices. If followed, it will lead to unnecessarily slower and less effective anti-abuse efforts.

It is highly appropriate for registry operators to suspend maliciously registered domain names – domain names registered by malefactors in order to carry out abuse. A registry can and should be both a first contact and first mover in such cases, and such suspensions do no harm to anyone except the abusers.

[83] "Sunrise to Sunset: Analyzing the End-to-end Life Cycle and Effectiveness of Phishing Attacks at Scale." 29th USENIX Security Symposium, August 12–14, 2020. https://www.usenix.org/system/files/sec20-oest-sunrise.pdf

These interventions are greatly needed. For example, research indicates that phishers themselves register half of the domain names on which phishing occurs.[84,85,86] These are domains that registry operators can suspend with great benefit to the public.

The need for registry operators to suspend maliciously registered domain names is the reason that Afilias established the first gTLD registry anti-abuse policy in 2008,[87] a policy adopted shortly afterwards by Public Interest Registry in 2009[88] and then by many new TLD operators from 2012 onwards. Registry operators such as Nominet, SIDN, and Afnic suspend domain names regularly, as a matter of good practice.[89] The latter have noted that "The distinction between [maliciously registered domains and compromised domains] is critical because they require different mitigation actions by different intermediaries. For example, hosting providers together with webmasters typically concentrate on cleaning up the content of compromised websites, whereas domain registries (*e.g.*, SIDN and Afnic) and registrars tend to focus on handling malicious domain name registrations."[90] Registries also have an "ideal vantage point" to detect problems, because they have a view across (often multiple) TLDs and can detect patterns of abuse that registrars cannot.[91] Registries also generally have greater capability due to their scale than registrars to perform such activities.

Nor have such suspensions proved to be risky or controversial in general. Registry operators such as Afilias, .XYZ, Neustar, .TK, and Nominet have suspended very large numbers of domains over time—totaling hundreds of thousands per year—with no real adverse consequences.

10.3.5 Dissent: Terms of Service

Section 1 states:

> One major barrier for providers to take action against abusive activity is that service providers' ability to address abuse is limited to their Terms of Service (ToS), barring legal orders presented by authorities in a relevant jurisdiction. Requesting actions outside

[84] "Phishing Landscape 2020: A Study of the Scope and Distribution of Phishing." pages 17-20 at http://www.interisle.net/PhishingLandscape2020.pdf

[85] G. Aaron and R. Rasmussen. "Global Phishing Survey: Trends and Domain Name Use in 2016." Anti-Phishing Working Group. https://docs.apwg.org//reports/APWG_Global_Phishing_Report_2015-2016.pdf

[86] Maroofi, M. Korczynski, C. Hesselman, B. Ampeau, A. Dud, "COMAR: Classification of Compromised versus Maliciously Registered Domains." 2020 IEEE European Symposium on Security and Privacy (EuroS&P). http://mkorczynski.com/COMAR_2020_IEEEEuroSP.pdf

[87] See https://afilias.info/news/2008/10/07/afilias-announces-new-policy-make-info-even-safer-internet-users and https://www.circleid.com/posts/20100924_afilias_excellence_online_trust_award_from_online_trust_alliance/

[88] https://gnso.icann.org/sites/default/files/filefield_26745/discussion-paper-rap-best-practices-28sep11-en.pdf

[89] For example see https://www.nominet.uk/over-28000-domains-suspended-as-law-enforcement-and-industry-keep-uk-safe/ and https://www.nominet.uk/law-enforcement-and-nominet-thwart-criminal-activity-online/ and https://www.sidn.nl/en/news-and-blogs/fake-webshops-taken-off-line-much-sooner

[90] See https://comar-project.univ-grenoble-alpes.fr/ and Maroofi, M. Korczynski, C. Hesselman, B. Ampeau, A. Dud, "COMAR: Classification of Compromised versus Maliciously Registered Domains." 2020 IEEE European Symposium on Security and Privacy (EuroS&P). http://mkorczynski.com/COMAR_2020_IEEEEuroSP.pdf

[91] For one example in action, see "Detecting and Taking Down Fraudulent Webshops at the .nl ccTLD. RIPE-NCC, 26 February 2020. https://labs.ripe.net/Members/giovane_moura/detecting-and-taking-down-fraudulent-webshops-at-a-cctld

> of those terms is asking a service provider to unilaterally break a contract with their customer. Terms of service for an operator allow the service provider to take actions to address abuse, but they are not a guarantee of action; there are still constraints on the service provider. Only where there is sufficient evidence to justify such an action, should an operator be expected to do so within the proper escalation path and timeframe. Thus, a provider's ToS are a key consideration for enabling effective anti-abuse outcomes.

and section 1.2.3 states:

> Evidentiary standards will ultimately be based on contractual terms, applicable law, and what is necessary for the service provider to enforce their terms of service and defend their actions.

These statements are partly true, but they imply that providers are often constrained by forces beyond their control. The reality is that many providers of Internet services are generally free to set their terms of service, and are then able to deal effectively and swiftly with abuse should they choose to. An example is GoDaddy, the world's largest registrar and a major hosting provider, which reserves the right to cancel user accounts and domain name registrations at "its sole and absolute discretion."[92] If a provider's terms of service are constrained, that is often the provider's own choice.

10.3.6 Alternative View: SSR2 Recommendation 13.1

Section 8 ("Findings") of the Report quotes this Recommendation from the SSR2 Review Team:

> 13.1 ICANN org should establish and maintain a central DNS abuse complaint portal that automatically directs all abuse reports to relevant parties. The system would purely act as an inflow, with ICANN org collecting and processing only summary and metadata, including timestamps and types of complaint (categorical). Use of the system should become mandatory for all generic top-level domains (gTLDs); the participation of each country code top-level domain (ccTLD) would be voluntary. In addition, ICANN org should share abuse reports (e.g., via email) with all ccTLDs.

Section 8 then draws the conclusion that the SSR2 statement is a "call for a centralized entity responsible for coordinated action.' We do not believe that the SSR2 recommendation is exactly a "call for a centralized entity responsible for coordinated action.' It recommends a central reporting and forwarding tool, but because ICANN would not be able to see the reports (just summary and metadata) it would not be able to use the tool for compliance purposes. Without complete data, neither ICANN nor this proposed system would be usable for any "coordinated

[92] "GoDaddy reserves the right, in its sole and absolute discretion, to suspend or terminate your Account..... Without limiting any of the rights set forth elsewhere in this Agreement, GoDaddy expressly reserves the right to deny, cancel, terminate, suspend, or limit future access to this Site or any Services (including but not limited to the right to cancel or transfer any domain name registration) to any User (i) whose Account or Services were previously terminated or suspended, whether due to breach of this or any other Agreement or any GoDaddy policy, or (ii) who otherwise engages or has engaged in inappropriate or unlawful activity while utilizing the Site or Services (as determined by GoDaddy in its sole and absolute discretion)." GoDaddy Universal Terms of Service Agreement, https://pk.godaddy.com/legal/agreements

action," and ICANN would not supplement other reporting options, nor could it become more "responsible" for abuse reporting and mitigation in the DNS space as a whole.

10.3.7 Dissenting SSAC Members

The following SSAC members join and support the Dissents and Alternative Views described in Sections 10.3.1 through 10.3.6:

Greg Aaron
Benedict Addis
Lyman Chapin
kc Claffy
Warren Kumari
John Levine
Mark Seiden

10.3.8 Alternative View: SSR2 Recommendation 13.1

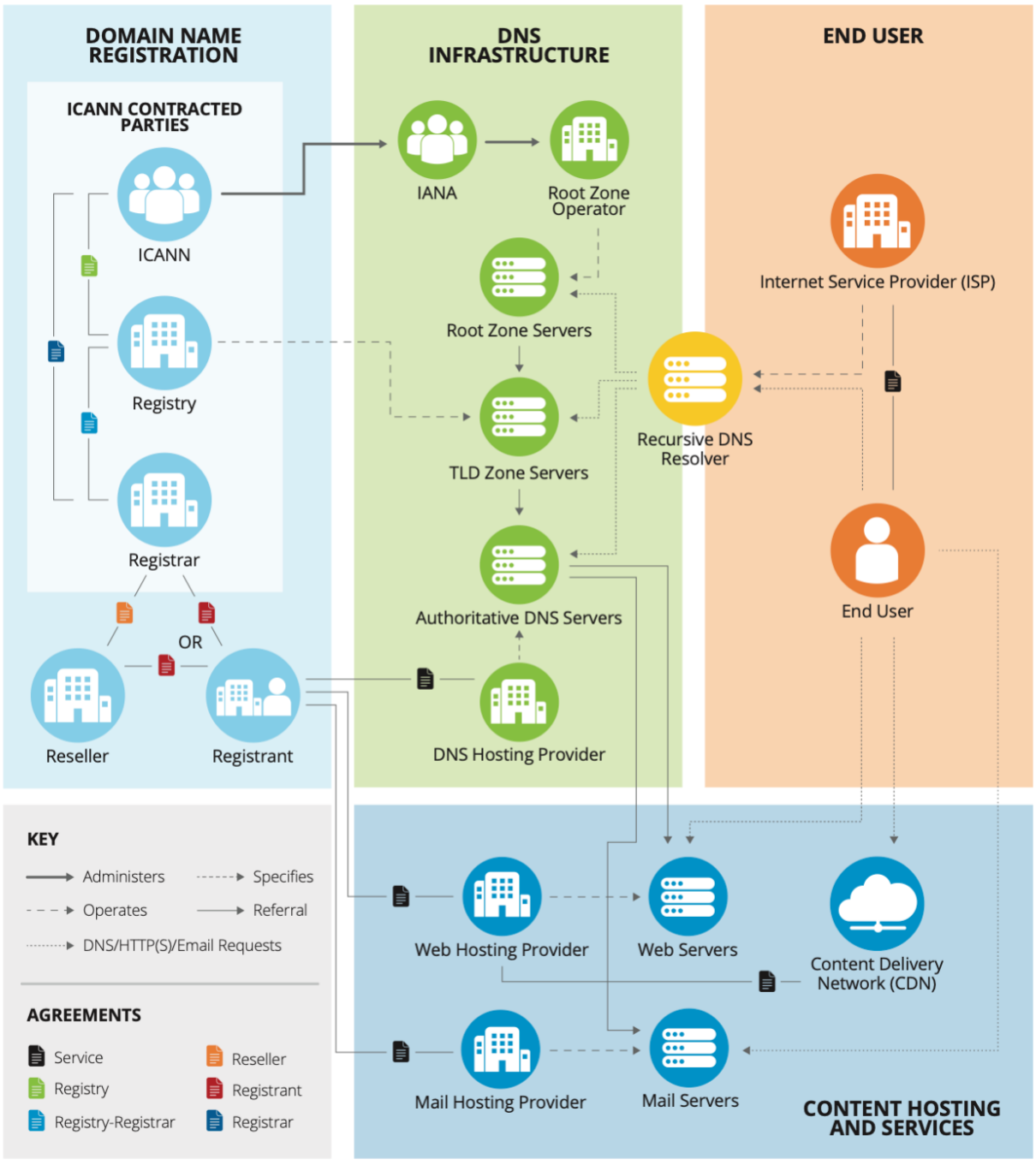
kc Claffy submits the following additional Alternative View concerning SSR2 Recommendation 13.1:

I agree with the Alternative View concerning SSR2 Recommendation 13.1 described in Section 10.3.6. As I served on the SSR2 review team, I can confirm this Alternative View's interpretation of that Recommendation. The confusion may be partly rooted in the fact that this Report takes a more expansive view of the DNS ecosystem, while SSR2 was required to deliver multi-stakeholder consensus on concrete, measurable recommendations strictly within ICANN's scope of responsibility.

10.4 Withdrawals

There were no withdrawals.

Appendix A: DNS Ecosystem



Conceptual Diagram of the DNS Ecosystem Portion Contractually Related to ICANN(image courtesy of Verisign)

Appendix B: Suggested primary party for abuse reporting/response

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	
DNS hosting infrastructure purchased to support abuse	DNS provider (DNS services purchased)	Registrar for domain Registry for domain DNS provider
DNS infrastructure registered to support abuse	Registrar for domain	Registry for domain DNS provider
DNS infrastructure compromised to support abuse	DNS hosting provider & Owner of domain name	Registrar of domain (for contacts)
Email account	Email service provider	ISP of origin
Other Internet service/protocol	Relevant service provider	ISP of origin

Appendix C: (Representative) Existing entities participating in the DNS Abuse Identification/detection problem space

Note: These entities operate do not have a contractual relationship with ICANN org and operate independent of the ICANN community

Organization/Entity Type	Problem Space Aspects Addressed	Roles	Type
Anti-Phishing Working Group (APWG)	E-crime - phishing, malware, fraud, criminal infrastructure, cryptocurrency abuse	● Operational information sharing ● Education ● Best practices ● Research ● Statistics/Trends ● Facilitate communications & networking	Non-Profit
Messaging, Malware, Mobile Anti-Abuse Working Group (M3AAWG)	E-crime & messaging abuse - spam (email, phone, SMS), phishing, malware, fraud	● Education ● Best practices & standards ● Research ● Public policy ● Statistics/Trends ● Facilitate communications & networking	Non-Profit
Phishtank	E-crime - phishing research	● Operational information sharing ● Research	Non-Profit (owned by Cisco)
Spamhaus, Surbl	E-crime	● Commercial detection and distribution of DNS abuse domains	Commercial (centralized reporting and publication)
	E-crime	● Commercial detection and distribution of DNS abuse domains	Commercial
Abusix	E-crime	● Commercial detection and distribution of DNS abuse	Commercial

Organization/Entity Type	Problem Space Aspects Addressed	Roles	Type
Phishlabs	E-crime	● Commercial detection and distribution of DNS abuse domains	Commercial
Malware Bytes	E-crime	● Commercial detection and distribution of DNS abuse domains	Commercial
(National Center for Missing and Exploited Children) NCMEC, In-Hope, Internet Watch Foundation (IWF)	Child sexual abuse material	● Incident response ● Law Enforcement ● Coordination of responses	Non-profit, quasi-governmental