Messaging, Malware and Mobile Anti-Abuse Working Group

M^{3}AAWG Input on ICANN's Next Abuse Policy Work

October 2025

Executive Summary

ICANN’s Generic Names Supporting Organization (GNSO) is currently considering ideas for a new policy-development process to address domain name abuse. It has recommended that a formal issues report be created to examine several ideas and their merits. M^{3}AAWG submits this discussion paper to the GNSO and the ICANN community as feedback. Below, we provide the perspective of anti-abuse professionals and researchers. M^{3}AAWG kindly requests that the following feedback be considered as ICANN’s Issues Report is written and considered.

Below we rank the ideas in our recommended order of preference, beginning with the ideas that have the highest value and descending to those with the lowest value. M^{3}AAWG believes that a policy placing limitations on bulk domain registrations has the greatest potential value.

Table of Contents

Introduction

The Messaging, Malware, and Mobile Anti-Abuse Working Group (M^3AAWG) is a global, technology-neutral industry association that develops cooperative approaches for fighting online abuse. Our more than 200 members form a diverse community across industry, government, academia, and civil society groups. M^3AAWG members are experts at fighting DNS abuses, including malware, spam, phishing, botnets, DoS attacks and other online exploitation. M^3AAWG has commented on a number of ICANN policy initiatives over the years.

Through the GNSO, the ICANN community is considering ideas to curb the abuse of domain names, with a goal of pursuing at least one new idea for focused policy-making. The GNSO's DNS Abuse Small Team recently created a report, and several other parties have proposed their own ideas.[1] This work is very important; the number of generic Top-Level Domain (gTLD) domain names being used for abusive purposes is in the millions per year.

Below, M^3AAWG evaluates these ideas based on the following criteria:

- Effectiveness: whether the idea is practical and will make a positive impact.
- Whether an idea will help *prevent* abuse, rather than focusing on response or mitigation. While response and mitigation are important, they happen after damage and victimization have occurred, and can have a limited effect on attackers, who often move quickly and cycle to fresh domain names.[2,3] Prevention and deterrence are more effective strategies than reactive enforcement.
- M^3AAWG believes that ICANN's efforts will be best spent on contractually binding requirements. Binding policies are applicable to all gTLD registrars and registry operators. In contrast, best practices are voluntary, unenforceable, and may not drive meaningful change.

Below, we rank the ideas in our recommended order of preference, beginning with the ideas that have the highest value and descending to those with the lowest value.

[1] **GNSO DNS Abuse Small Team**: https://gnso.icann.org/sites/default/files/policy/2025/draft/dns-abuse-small-team-report-04aug25-en.pdf
ICANN Government Advisory Council (GAC): https://gac.icann.org/contentMigrated/icann83-prague-communique
NetBeacon Institute proposals: https://netbeacon.org/white-paper-proposal-for-pdps-on-dns-abuse/
ICANN Contracted Parties House proposals: https://icann83.sched.com/event/246R0/gnso-cph-dns-abuse-community-update

[2] ICANN Office of the CTO: "Insights and Clarifications on the INFERMAL Study." 10 June 2025. https://www.icann.org/en/system/files/files/insights-clarifications-infermal-study-10jun25-en.pdf

[3] "M^3AAWG DNS Abuse Prevention, Remediation, and Mitigation Practices for Registrars and Registries," January 2024. https://www.m3aawg.org/sites/default/files/dns_abuse_prevention_remediation_and_mitigation_practices_for_registrars_and_registries.pdf

#1 Proposal: Limits on Bulk Registrations and API Access

Concept: Create requirements that make it more difficult for parties to register significant numbers of domain names. Some parties have referred to this idea as limits on "API access." A policy could require registrars to positively verify the identities of registrants who wish to register more than a certain number of domain names.[4]

M^{3}AAWG conclusion: this idea offers significant opportunities for abuse prevention. Of the ideas under discussion, this idea has the highest potential value for ICANN policy-making.

Background:

1. Cybercriminals often register large numbers of domain names, and in an automated fashion.[5] This allows them to launch large numbers of attacks and to stay ahead of mitigation efforts.
2. APIs enable bulk, automated registration and configuration, a capability heavily exploited by attackers.[6]
3. Bad actors sometimes register domains through resellers, and occasionally become resellers themselves in order to gain access to automation tools and registration APIs.[7]
4. M^{3}AAWG members observe millions of malicious domain name registrations made in bulk in the gTLDs every year.
5. The significant scale of the problem justifies a risk-based approach.

[4] **ICANN GNSO Small Team**: "Unrestricted API access for domain name registration for new customers: Some studies and other community inputs indicate a possible correlation between abuse and unrestricted API-enabled domain name registrations."
ICANN Government Advisory Council (GAC): "The GAC advises the Board: i. To urge the GNSO Council to undertake all necessary preparations prior to ICANN84 towards starting targeted and narrowly scoped Policy Development Processes (PDPs) on DNS Abuse issues, prioritizing bulk registration of malicious domain names and the responsibility of registrars to investigate domains associated with registrant accounts that are the subject of actionable reports of DNS Abuse."
NetBeacon Institute: "Friction in Bulk Registrations for New Customers: A proactive approach that seeks to introduce friction for new customer accounts, prior to gaining access to high volume registration tools (i.e., API access for new customers), until trust is established."
ICANN Contracted Parties House: "API/reseller Agreement Mandatory Clauses."

[5] Interisle Consulting Group: "Cybercrime Supply Chain 2024 Report," 18 November 2024, pages 26-29. https://interisle.net/s/CybercrimeSupplyChain2024-wyf6.pdf

[6] ICANN Office of the CTO: "Insights and Clarifications on the INFERMAL Study."

[7] At ICANN83, the ICANN Contracted Parties House posed the question: "Could the requirements of the Registrar Accreditation Agreement (RAA) regarding use of resellers be improved with an advisory to clarify the reseller obligations with respect to DNS abuse mitigation? Section 3.12 of the RAA could be improved to ensure registrars that offer an API/Reseller program have the necessary contractual means to impose DNS mitigation requirements on their resellers." M^{3}AAWG notes that ICANN's Registrar Accreditation Agreement (section 3.12) already makes these obligations clear. It requires registrars to make sure that their resellers comply with all ICANN obligations, including anti-abuse requirements. This obligation should be maintained.

6. M^{3}AAWG recently urged ICANN to implement enforceable contractual terms to prevent systemic abuse and malicious bulk registrations.[8]
7. M^{3}AAWG has documented anti-abuse best practices that registrars and registry operators can use to prevent bulk registrations, and to address contributing vectors such as fraudulent account creation and payment fraud.[9]

M^{3}AAWG assumptions and comments:

A. The problem is that *bad actors easily register and use large numbers of domains*. The purpose of this policy should be to *prevent bad actors from obtaining large numbers of domains*.

B. "APIs" or "access to APIs" are an aspect of the problem, and are how some of this abuse is carried out, but "access to APIs" is not exactly the problem itself, and "limiting access to APIs" is not the entire solution. An ICANN policy should recognize that APIs are often a tool used somewhere in the process, but just "restricting access to APIs" will not solve the problem, and may have loopholes.[10]

C. There are parties who register large numbers of domains for allowable reasons (e.g., domain speculation and defensive registrations). A policy must allow those parties to make registrations. However, given the scale of abuse associated with malicious bulk registrations, imposing some friction – even upon legitimate registrants – is a reasonable, risk-based approach.

D. To make prevention effective, there will need to be clear, enforceable standards for how a registrar can determine if a registrant is trustworthy and can be allowed to make bulk registrations.

E. The definition of "bulk registration" must prevent gaming by bad actors. It is common for bad actors to use evasion techniques. They use multiple accounts at a registrar, sometimes register every domain to a different registrant name, and register multiple small batches of domains spaced by time, with the ultimate aim of amassing large numbers of domains.

F. If a registrant uses domains for abusive activities, the policy should require the registrar to suspend all registrations made by the bad actor and to cease doing business with that party. There should, of course, be an exception if the registrant is innocent and has had their account compromised.

[8] "Comments of the Messaging Malware Mobile Anti-Abuse Working Group (M^{3}AAWG) on ICANN Amendments to the Base gTLD RA and RAA to Modify DNS Abuse Contract Obligations," 12 July 2023. https://www.m3aawg.org/sites/default/files/m3aawg_comments_on.dns_abuse_contract_obligations.docx_.pdf

[9] "M^{3}AAWG DNS Abuse Prevention, Remediation, and Mitigation Practices for Registrars and Registries." January 2024. https://www.m3aawg.org/sites/default/files/dns_abuse_prevention_remediation_and_mitigation_practices_for_registrars_and_registries.pdf

[10] For example, some registrars offer the ability to register large numbers of domains (up to 5,000 at a time) via their web site interfaces. And some criminals automate registrations through registrar web interfaces that offer a small number of domains at a time, thereby circumventing those limits and obtaining large numbers of domains. In these cases the registrant does not interact directly with an API at all. (The registrar may send the data via one or more APIs that make transactions in registries. Here the registrar is the only party with direct API access to a registry.)

Effectiveness:

- This idea has a high potential for preventing abuse.
- The effectiveness of the policy will depend upon implementation by registrars.
- Of the ideas under discussion, this idea has the highest potential value for ICANN policy-making.

#2 Proposal: Bulk Access to Domain Registration Data

Concept: Provide bulk access to the publicly available domain registration data for all gTLD domains. Doing so would make it easier for security responders and researchers to obtain access to the data they need at scale, while simultaneously reducing the query load on registry and registrar Registration Data Access Protocol (RDAP) and WHOIS servers.

This is a new idea proposed by M^{3}AAWG members. Since it is about registration data, it might be suitable to pursue at ICANN on a different track than the other anti-abuse ideas under discussion. M^{3}AAWG finds this idea to be of high value.

Background:

1. Domain registration data is essential for security and anti-abuse purposes.[11] Security companies and researchers, including a number of M^{3}AAWG members, need it to track millions of gTLD domain names each day. This includes data only available through RDAP and WHOIS queries, such as Sponsoring Registrar, Create Date, Registrant Country, and Extensible Provisioning Protocol (EPP) statuses.
2. This requires, in the aggregate, many millions of queries per day. The number of RDAP and WHOIS queries made to the .COM registry alone is *28 billion per month*.[12] Making these queries is burdensome for security practitioners, and responding to their domain-by-domain queries places demand on registries' and registrars' systems.
3. Many registrars and registry operators limit access to the public data by imposing *rate limits* at their RDAP and WHOIS servers. Rate-limiting prevents security practitioners from finding and monitoring abusive domains.[13] At the rate-limits currently being imposed in the industry, most users of RDAP and WHOIS can only observe a fraction of the activity taking place in many TLDs and registrar portfolios.

[11] See "Recommendations pertaining to findings from the M^{3}AAWG and APWG WHOIS Survey Report presented to ICANN in June, 2021", https://www.m3aawg.org/sites/default/files/icann_recommendations_whois_survey_report-sept302021.pdf
See also: https://www.m3aawg.org/sites/default/files/icann-epdp-phase-2a-final-report-comments-jan62022.pdf

[12] See .COM Activity Reports, https://www.icann.org/resources/pages/com-2014-03-04-en

[13] For information about what rate limits are, how they are imposed, and the challenges they pose for security and stability purposes, see: ICANN Security and Stability Advisory Committee: *SAC101v2: SSAC Advisory Regarding Access to Domain Name Registration Dat*a, https://itp.cdn.icann.org/en/files/security-and-stability-advisory-committee-ssac-reports/sac-101-v2-en-14-11-2023-en.pdf

4. Many parties benefit when security professionals have the data they need. This includes not only the public, which is better protected, but also registrars and registry operators, who receive abuse reports from security professionals, alerting them to bad customers.

M^{3}AAWG assumptions and comments:

A. ICANN's Centralized Zone Data Service (CZDS[14]) provides a model. It is a place where parties can apply to receive gTLD zone files. In a similar fashion, parties could apply to receive files containing gTLD domain data, updated once per day.
B. This idea does not pose privacy issues. It would simply make data that is already publicly available accessible via another means.
C. Registry operators must be required to participate. They would provide data about all domains in the gTLD registry, updated once per day.
D. The contact data that is publicly available in registrar Registration Data Directory Services (RDDS) output is highly useful for security and anti-abuse purposes, and should be made available via bulk access.
E. Therefore, registrars should also participate, providing bulk data about the gTLD domains in their portfolios. This is necessary since ICANN's new data policy[14] has allowed fragmentation, where some domain records in a given registry are "thick" and others are "thin;" also .COM and .NET remain thin, and the registrars are the only source of contact data.
F. Registrars and registry operators must continue to make registration data services available via RDAP, under current service-level agreements (SLAs). . Bulk access is proposed as an alternate means to obtain the data, but not as a replacement for RDAP service.
G. Applicants requesting bulk access would briefly describe the purpose for making their data request, much as CZDS zone data requestors currently do.

Effectiveness:

- M^{3}AAWG finds this idea to be of high value, and practical.

[14] https://www.icann.org/en/contracted-parties/consensus-policies/registration-data-policy

#3 Proposal: Investigate Associated Domains

Concept: registrars and registry operators would be required to investigate other domains associated with identified abuse domains linked to the same actor.[15]

M^{3}AAWG conclusion: This idea has some merit because it could help with both prevention and mitigation. However, its efficacy will depend upon diligent and professional execution, and it poses some enforcement and compliance challenges.

Background: The ICANN Contracted Parties House says the potential value is that "it may contribute to mitigating or disrupting other malicious registered domains in the same registrant account."

M^{3}AAWG assumptions and comments:

A. The goal of this process is to address the *bad actor* perpetrating abuse and to suspend all domain names associated with that bad actor (customer).

B. Bad actors use techniques to evade detection. For example, they use multiple accounts at a registrar, multiple registrant names, and varying payment methods. Another issue is that one domain holder (and one registrant identity) can be associated with multiple EPP contact objects. The policy should not require that just the domains associated with one registrant contact ID or account be investigated.

C. Therefore, for this policy to be effective, registrars and registry operators must be diligent and effective at linking bad actors to their domains.

D. To be effective, the policy should be applied to registrars and registry operators. The registrar possesses the most data on which to perform investigations and "pivots" – including account data, billing data, and the actual registrant contact info. Only a registry operator can investigate patterns across registrars.

E. In cases of abuse, registrars and registry operators should be required to *take action* against relevant associated domains and the account(s) involved.

F. A new policy would focus on malicious registrations – domains registered for the purpose of committing abuse. Registrars and registry operators should not be required

[15] **ICANN GNSO Abuse Small Team**: "there is currently no contractual requirement or best practice standard requiring contracted parties to investigate domains associated with known malicious actors."
ICANN Government Advisory Council (GAC): "The GAC advises the Board: i. To urge the GNSO Council to undertake all necessary preparations prior to ICANN84 towards starting targeted and narrowly scoped Policy Development Processes (PDPs) on DNS Abuse issues, prioritizing bulk registration of malicious domain names and the responsibility of registrars to investigate domains associated with registrant accounts that are the subject of actionable reports of DNS Abuse."
NetBeacon Institute: "A reactive approach requiring registrars to investigate domains linked to malicious actors, particularly in cases of bulk domain registrations used for abuse campaigns."
ICANN Contracted Parties House: "Should registrars have a requirement to inspect other domains in a customer account, or attached to the same registrant information, when they are investigating an actionable DNS abuse report?"

to suspend compromised domains or to penalize innocent registrants who have had their accounts compromised by criminals.

Effectiveness:

- The efficacy of this idea depends on effective investigations and execution by the registrars and registry operators.
- This idea offers some prevention value. It could prevent some domains from being used by bad actors.
- The enforcement of such a policy will require a level of sophistication from ICANN's Compliance Department. ICANN would need to request relevant data when investigating complaints.

#4 Proposal: Subdomain DNS Abuse

Concept: "[H]elp address the growing abuse of subdomain services by codifying the responsibilities of registrants who offer them, via requirements in registrar and registry terms of service."[16]

M^{3}AAWG conclusion: This subject might be outside ICANN policy-making scope, and ICANN is not able to provide a comprehensively impactful solution.

Background:

1. Subdomain services give customers a third-level domain on a second-level domain name that the provider owns. This gives users their own DNS space, on a hostname of the format: *subdomain.domainname.tld*. Some of these providers offer website building or hosting services; others offer free DNS management so the customer can point the hostname to other hosting.
2. Phishers notably use these services to build and maintain phishing sites, and they are used to perpetrate other kinds of abuse.
3. The use of subdomain services for phishing is significantly concentrated on fewer than 100 second-level gTLD domain names. These domain names are operated by a small number of companies, and 90% of the related phishing attacks occurred on domains operated by just ten companies.[17]

[16] Proposed by NetBeacon Institute.

[17] For a list of domains and their operators, and statistics about the use of subdomain services for phishing, see: Interisle Consulting Group, *Phishing Landscape 2024: A Study of the Scope and Distribution of Phishing*, pages 17-20. https://static1.squarespace.com/static/63dbf2b9075aa2535887e365/t/66cde404c8345e766972319c/1724769286084/PhishingLandscape2024.pdf and *Phishing Landscape 2025: A Study of the Scope and Distribution of Phishing*, pages 18-20. https://interisle.net/insights/phishing-landscape-2025-an-annual-study-of-the-scope-and-distribution-of-phishing

M^{3}AAWG assumptions and comments:

A. M^{3}AAWG believes that the abuse of these services is a significant issue. However, we do not rank this as a priority for ICANN policy-making. We also see some issues that might prevent ICANN from creating effective, binding solutions.
B. Before embarking on a policy-development process on this idea, ICANN should first determine if it is within ICANN's policy-making remit. Section 1.1 of ICANN's Bylaws states that ICANN's mission is that it "coordinates the development and implementation of policies concerning the registration of *second-level* domain names" [emphasis added].[18] ICANN has never made policies for providing or managing *third-level* domains.
C. To be effective, ICANN would need to declare new, legally binding requirements upon any party that will or already provides third-level gTLD domains to other parties. Presumably, this would be done by "flowing down" the requirements through the Registrar Accreditation Agreement (RAA) and the registrar-registrant contract.
D. Who could or would enforce contractual requirements on a third-level domain provider?
    a. ICANN does not perform direct contract compliance on registrants. In this case, the third-level domain providers are registrants.
    b. "Contractual flow-down" means that registrars would be responsible for providing compliance oversight upon the third-level providers. But that appears to be unworkable. Registrars and registry operators cannot take any direct action to mitigate or prevent abuse on subdomains. The only effective compliance action they could take would be to suspend the second-level domain. However, these second-level domains should not be suspended, because doing so would disrupt the legitimate users who are using third-level domains on them. Only the subdomain providers can mitigate harm on their services, by suspending third-level domains.
E. Some of the second-level domains used are in country code top-level domain (ccTLDs), over which ICANN has no control. This would prevent ICANN from creating a comprehensively effective, binding solution.
F. A new ICANN policy would only affect a very small number of registrants.
G. Subdomain abuse is essentially an issue of how companies choose to make their services available: such as whether they make subdomains available for free, whether sign-up is easy or there is some friction in the process, and how well they respond to abuse complaints. It is unclear if, or how, ICANN could force them to behave differently.
H. The providers of third-level domains are well aware of the abuse occurring on their domains. They receive thousands of professional abuse reports per month about their

[18] https://www.icann.org/en/governance/bylaws#article1

subdomains from security responders (including a number of M^{3}AAWG members), and their subdomains appear on the major DNS blocklists.

Effectiveness:

- For the reasons above, it may not be practical for ICANN to make policy here, and M^{3}AAWG does not recommend it be a priority.

#5 Proposal: Centralized Coordination for Domain Generation Algorithms (DGAs)

Concept: Create a centralized coordination function to block domains used by botnets and malware that rely on domain generation algorithms (DGAs).[19]

M^{3}AAWG conclusion: ICANN does not have the ability to create an effective solution.

Background:

A. A DGA is a program that generates large numbers of new domain strings; any one of them (once registered by the malefactor) can be used to control the botnet or malware. Cybercriminals use DGAs to make mitigation difficult for defenders and use them to frequently change the domains they use.

B. Preemptively blocking or registering all of the generated ("viable") domains will prevent the malware or botnet from receiving new instructions, effectively preventing it from functioning. But if *all* of the generated domains are not blocked, then the malware or botnet can continue to be controlled by its operator.

C. This type of work has been addressed by various players over the years, including entities such as ShadowServer and ad-hoc security groups.

D. Dangerous or impactful botnets tend to attract the attention of law enforcement.

E. Each DGA event tends to be unique, and defensive and reactive processes often need to be tailored.

[19] **ICANN GNSO Abuse Small Team**: "Limited coordination on DGA-based abuse: The current system for responding to Domain Generation Algorithm (DGA)-based threats commonly used in botnets and malware campaigns seems to be fragmented. No single trusted platform or voluntary protocol for real-time information sharing between registries, registrars, and law enforcement means fragmentation causing delays and inconsistent responses."
NetBeacon Institute: "A proposal to have ICANN serve as a coordination hub for law enforcement and national CERTs in cases involving DGA-based malware and botnets, enabling more efficient, synchronized mitigation."
ICANN Contracted Parties House: "Mitigation of Batch Registered Domain Names Generated by a Botnet Algorithm." "Should there be a clearinghouse to verify DGA lists that can be distributed to gTLD registry operators pursuant to DNS Abuse Mitigation Obligations? If so, who can function as the clearinghouse? What functions would this clearinghouse perform?"

F. While DGAs are a vexing tool used by cybercriminals, the number in active use, and how often new ones appear, has not been well documented.[20]

Effectiveness:

1. DGAs often use ccTLD domains, and can use ccTLD domains exclusively. Unless ccTLD domains are addressed, the malware or botnet will have the ability to continue to function, and blocking in just gTLDs will be fruitless. ICANN cannot create a policy that compels ccTLD participation. Therefore, this is an area in which ICANN policy-making cannot deliver a fully effective solution.
2. ICANN Org seems unsuited to act as the central coordinator for anti-DGA work. In the past, ICANN participants have not seen ICANN as an operational hub, network operations center (NOC), or Information Sharing and Analysis Center (ISAC).
3. If a central coordination entity is stood up but not under ICANN's control, it will not have any compulsory authority. (Unless ICANN requires its registrars and registry operators to take mandatory direction from that third party, for example requiring registries to suspend or block lists of domains that the central coordinator provides.)
4. Standing up a dedicated third-party entity to be the central coordinator raises other challenges, such as funding.
5. DGAs are used by a small number of actors. Other anti-abuse policies could hinder the activities of a more diverse set of malicious actors, who collectively use larger numbers of domains.

#6 Proposal: Registrant Recourse Mechanisms

Concept: "A measure that ensures registrants have a path to challenge enforcement actions of registrars or registries when taken in error."[21]

M^{3}AAWG conclusion: This idea is not designed to prevent or mitigate abuse. The need for a policy has not been justified, and a policy could be abused if not written properly.

Background:

A. This is a customer relationship and service function between registrars and registrants. Registrants already have appeals processes at their registrars, which have been traditionally handled under registrar terms of service.

[20] For example, the existence of 22 DGAs has been documented in the MITRE repository since 2008, with no new ones documented there since 2022. See https://attack.mitre.org/techniques/T1568/002/ . MITRE ATT&CK® is a prominent knowledge base of adversary tactics and techniques. It is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

[21] Proposed by NetBeacon Institute.

B. There is no demonstrated need for a new ICANN process here, and existing processes apparently work well. Registrars and registry operators have been suspending large numbers of domains for twenty years. Anecdotal evidence suggests that the number of false positives (domains mistakenly suspended for abuse) and the resulting impacts are very small.

C. M^{3}AAWG does not discount the harm that can be caused when a domain name is suspended by mistake, due to no bad behavior on the part of the registrant, and has always recommended that domain suspensions be carried out professionally.[22]

D. M^{3}AAWG members operate blocklists, and regularly receive bogus de-listing requests from cybercriminals. A poorly written policy could allow bad actors to use an appeals process to hold up necessary suspensions.

Effectiveness:

1. This idea is not effective and it will not help prevent or mitigate abuse.

Conclusion

M^{3}AAWG thanks the GNSO, ICANN Org, and other ICANN community members for considering this document. Among the ideas currently under consideration, the idea of restricting bulk registrations of domains has significant potential to reduce DNS abuse and the highest potential value for ICANN policy-making.

M^{3}AAWG also remains interested in ideas that will make domain registration data more readily available to security professionals, to the full extent allowed by law.

We appreciate the opportunity to submit these comments and welcome further opportunities to engage as needed to answer any questions during this process. Please address any inquiries to M^{3}AAWG Executive Director Amy Cadagin at comments@m3aawg.org.

Sincerely,
Amy Cadagin
Executive Director
Messaging Malware Mobile Anti-Abuse Working Group (M^{3}AAWG)
P.O. Box 9125, Brea, CA 92822
comments@m3aawg.org

[22] "M^{3}AAWG DNS Abuse Prevention, Remediation, and Mitigation Practices for Registrars and Registries." January 2024. https://www.m3aawg.org/sites/default/files/dns_abuse_prevention_remediation_and_mitigation_practices_for_registrars_and_registries.pdf