The ICANN GNSO "Business Constituency"

ICANN Business Constituency (BC) Comment

on

Amendments to the Base gTLD RA and RAA to Modify DNS Abuse Contract Obligations

20-Jul-2023

This document is the response of the ICANN Business Constituency (BC), from the perspective of business users and registrants, as defined in our Charter. The mission of the BC is to ensure that ICANN policy positions are consistent with the development of an internet that:

- Promotes end-user confidence, because it is a safe place to conduct business;
- Is competitive in the supply of registry- and registrar-related services; and
- Is technically stable, secure and reliable.

The BC greatly appreciates the efforts of contracted parties and ICANN Org for their good-faith negotiations on amendments to the Registrar Accreditation Agreement (RAA) and base gTLD Registry Agreement (RA) on the important issue of DNS Abuse. These proposed amendments are a good first step, represent meaningful progress, and will serve as a solid foundation for what we hope will be a long-term effort by industry to address this persistent and evolving problem. We respectfully suggest a few additional targeted improvements to the proposal to ensure that the worst cases of DNS abuse are effectively mitigated in a timely manner by **all** contracted parties.

Section 1 of our comment conveys the BC position, highlights areas for improvement, and provides suggestions for next steps to advance this issue. In the second section, we suggest edits and provide comments on the May-2023 draft **Advisory: Compliance With DNS Abuse Obligations in the Registrar Accreditation Agreement and the Registry Agreement**[1]

Areas for Improvement:

- **DNS Abuse Involving CSAM**: We recommend immediate consideration of how distribution of child sexual abuse material (CSAM) could be addressed at the DNS level.
- **Actionable Evidence of DNS Abuse**: The proposal limits actionable evidence to when a domain name "**is being used for DNS Abuse",** but this should be expanded to include reference to when there is actionable evidence that the domain name "**was used"** for DNS Abuse". This change would help prevent the domain name from jumping from one hosting provider to another to continue the abusive behavior.
- **Affirmative obligation for registry mitigation**: The proposed amendments require registry operators to refer abuse reports to the appropriate registrar(s), ***but do not require the registry to act* to mitigate** in the event the registrar does not. There will be instances of non-action by registrars which might require registry action, so referring the abusive domain name to the sponsoring registrar would be inadequate. We encourage text that more closely mirrors the obligations of the registrar in terms of interrupting DNS abuse. The BC suggests the proposal would be improved if it

[1] See https://itp.cdn.icann.org/en/files/registry-agreement/draft-icann-advisory-dns-abuse-amendments-25-05-2023-en.pdf

required the registry to take mitigation action *when the registrar does not*.

- **Response timeframes**: The BC is concerned about a lack of specific timeframes to respond to abuse threats, not taking into account the urgent nature of some of those threats and potentially making it difficult for ICANN Compliance to enforce. Accordingly, the BC advocates a service-level agreement (SLA) that guarantees timely reactions to abusive behavior. Specifically, because threats can emerge and cause damage within minutes or hours, we suggest action within no later than 48 hours from receipt of a credible threat report, absent extenuating circumstances.
- **Required responses to abuse reports**: It would be particularly helpful if registries and registrars were required to clearly document to the abuse reporter the specific steps taken (or in some instances, not taken) to address reported abuse. Such a requirement not only would help "close the loop" on reported abuse, but would help refine reporting procedures over time, making them more focused and efficient. We are cognizant of potential privacy concerns associated with this, and request that this matter be looked into so as to benefit all involved parties.
- **Empowerment of ICANN Compliance**: The BC has been long concerned over the capability of the ICANN Compliance department to enforce against registrars and registries that intentionally harbor abuse. Accordingly, the BC is interested in advancing avenues for Compliance to take action against contracted parties with truly out of the curve, unacceptably high, rates of malicious domain name registrations, calculated as a percentage of their overall registrations.

Advisories:

- **Contract language and placement**: The BC suggests that much of the proposed amendment language housed in supplemental documents (or elsewhere, away from the main provisions of the contracts) be incorporated into the contracts themselves in order to remove the potential for misinterpretation or unintentional lack of enforceability.
- **Abuse at scale**: The proposed amendments unfortunately do not address the critical issue of *scale* – that is, abuse that all too often is carried out by one party across multiple domain names. Contracted parties and ICANN Org would be much better situated to efficiently mitigate abuse if they have the means to do so -- not on a one-by-one basis, but at the "party" or "account" level, with the capability of addressing broad swaths of abuse at one time. The BC favors language to address this capability, or at a minimum, to request that ICANN issue advisories to contracted parties regarding methods for handling systemic abuse *at scale*.
- **Concerns Regarding Abuse Contact Emails (3.18.1).** The BC notes that email addresses designated for abuse reporting often are filtered or subject to spam collection. Accordingly, the proposed amendment could be updated to ensure that such addresses are properly designated, configured and manned for optimum review and response times. This would ensure that webforms do not impose unreasonable rate or size limits, allow file attachments, and permit other procedures that allow abuse reporting submissions to be complete and correct. The BC is in favor of language to address this issue, or at a minimum, to request that ICANN issues advisories to contracted parties to address these concerns.
- **Clarification of and what is meant by "respond appropriately to any reports of abuse."** The BC is concerned about ambiguity in the existing language that is not sufficiently defined, but should be in order to carry proper effect. The BC is in favor of language to address this issue, or at a minimum, to request that ICANN issues advisories to contracted parties to address these concerns.

Areas for Subsequent Work:

- **Definition of DNS abuse (3.18.1)**: The BC consistently has agreed with its ICANN colleagues in the Security and Stability Advisory Committee (SSAC) that the definition of DNS abuse should not be regarded as static, as threat vectors evolve over time; abuse definitions, therefore, must evolve as well. We respectfully request that ICANN Org discontinue citing SAC115 as the "source" of its working definition of DNS abuse when, in fact, we believe the definition originates from the contracted parties' Voluntary Framework on DNS Abuse.

  The BC accordingly refers to SAC115 as follows:
  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 provide a general definition of abuse that may accommodate the evolving natures of abuse and cybercrime over time.*** (Emphasis added)

  The BC is on record in multiple fora stating that this definition is – over the long term – insufficient. While the BC appreciates the initial definition for purposes of dealing with specific forms of abuse, the definition does not take into account other well-known forms of damaging behavior. This definition should not remain static and must be subject to periodic community review. We suggest a regular independent review of the definition of DNS abuse, with an eye toward incorporating reasonably anticipated changes in sources of abuse.

- **Ongoing *prevention* of DNS abuse from known abusers**: While the proposed amendments are focused on mitigation of DNS abuse *after* it has occurred, the BC sees an additional opportunity within the contracts to *prevent* abuse from occurring. As noted above regarding addressing abuse at the "account" level, registrars should be required to suspend or terminate a customer account after a defined number of reported and verified cases of abuse. In such instances, registrars could be obligated to cooperatively share data regarding known perpetrators of abuse, preventing those persons or entities from launching new efforts to use the DNS for abusive purposes across multiple providers. The BC favors a micro-PDP on this topic as a possible next step for future work.

Next Steps
We respectfully submit these recommendations for consideration – either in the current proposal, or if not feasible to address now, in future opportunities to improve the contracts, such as the next round of gTLDs.

In the next section, we suggest edits and provide comments on the May-2023 draft **Advisory: Compliance With DNS Abuse Obligations in the Registrar Accreditation Agreement and the Registry Agreement**[2]**.** Please be sure to view the comments embedded in the Microsoft Word markup of the Advisory.

This comment was drafted by Margie Milam, Mark Datysgeld, Crystal Ondo, and Mason Cole. It was approved in accord with our charter.

[2] See https://itp.cdn.icann.org/en/files/registry-agreement/draft-icann-advisory-dns-abuse-amendments-25-05-2023-en.pdf

Advisory: Compliance With DNS Abuse Obligations in the Registrar Accreditation Agreement and the Registry Agreement

Commented [A1]: See comments below regarding this Advisory. However, as noted in BC comments on the RAA/RA amendments themselves, the BC suggests that any clarifications outlined in this Advisory or other external documents be incorporated directly into the RA/RAA themselves to remove the potential for misinterpretation or unintentional lack of enforceability.

This Advisory provides guidance on the interpretation of and compliance with the [DATE] amendments to the Registrar Accreditation Agreement (RAA) and the Base Generic Top-Level Domain (gTLD) Registry Agreement (RA) regarding Domain Name System (DNS) Abuse mitigation obligations (DNS Abuse Amendments).

Unless specifically modified by the DNS Abuse Amendments, all RAA and RA obligations that were in effect prior to these Amendments remain applicable and in force.

All capitalized terms that are not defined in this Advisory have the meanings given to them in the RAA and the RA.

Registrars and registries that use the practices set forth in this Advisory would likely meet the obligations set forth in the DNS Abuse Amendments, but adherence to one or more of these practices will not automatically result in a determination that the registrar or registry operator has complied with its obligations. The examples set forth below are illustrative only and are not intended to limit the possible mitigation actions. In all cases, whenever ICANN Contractual Compliance initiates an investigation, registrars and registry operators must provide evidence demonstrating compliance with the relevant RAA and RA requirements.

Background

The ICANN organization contracts with registries to operate gTLDs through an RA. The RA specifies the responsibilities of the registry operator, which include maintaining the authoritative database of all registered domain names in the gTLD and publishing the DNS zone for the gTLD.

ICANN also enters into an RAA with each registrar, which allows the registrar to offer domain name registration services in gTLDs. The RAA outlines the responsibilities of

the registrar, such as verifying registrant (or Registered Name Holder) information and maintaining accurate registration records. The roles and obligations of registrars and registries are distinct and are reflected in their respective agreements, the RAA and the RA.

ICANN has the authority to enforce rules related to domain name registration services and domain names as outlined in the RAA and the RA. This Advisory focuses on domain names (or Registered Names) in gTLDs that are used as vehicles or mechanisms for DNS Abuse. The requirements of the DNS Abuse Amendments in the RAA and RA are based on the actions that registrars and registry operators, respectively, can take to minimize the scope and intensity of the harm and victimization caused by DNS Abuse. These requirements also consider that registrars and registry operators represent only a portion of the DNS ecosystem, which is composed of many actors[1]. Depending on the specific circumstances of an instance of DNS Abuse, the most appropriate actor to detect, assess, verify, and/or stop the abusive activity may vary, and sometimes may be an actor other than a registrar or registry operator.

DNS Abuse

For the purposes of the RAA, the RA, and this Advisory, *DNS Abuse* means malware, botnets, phishing, pharming, and spam (when spam is used as a delivery mechanism for any of the other four types of DNS Abuse) as these terms are defined in Section 2.1 of the Security and Stability Advisory Committee Report on an Interoperable Approach to Addressing Abuse Handling in the DNS (SAC 115[2]):

> **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.

Commented [A2]: As discussed in comments on the RAA and RA amendments themselves, the citation to SAC 115 for this definition is somewhat misplaced, as the definition actually originates from the Voluntary Framework on DNS Abuse (it is merely discussed in the SAC 115 report). Further, as noted in the comments on the amendments themselves, while the BC appreciates the initial definition for purposes of dealing with specific forms of abuse, the definition does not take into account other well-known forms of damaging behavior (e.g., child sexual abuse material, the online sale of pharmaceuticals without a prescription, etc.). If DNS abuse is to be meaningfully handled, this definition should not remain static and must be subject to periodic community review.

[1] Additional information can be found in the report produced by the DNS Abuse Special Interest Group at FIRST, which also includes advice for incident response teams on the organizations that might be productively contacted at different incident response phases for different DNS abuse techniques.
In addition, the Internet and Jurisdiction Policy Network (https://www.internetjurisdiction.net/) has provided further guidance on these forms of DNS Abuse in its "Operational Approaches, Norms, Criteria, and Mechanisms."

[2] ICANN Security and Stability Advisory Committee's SAC 115, Section 2.1, Pages 12–13, 19 March 2021

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 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 is sent as part of a larger collection of messages, all having substantively identical content. Spam is only considered to be DNS Abuse when it is being used as a delivery mechanism for at least one of the other types of DNS abuse described above.

Registrar Obligations

Section 3.18 of the RAA

Prior to the enactment of the DNS Abuse Amendments, Section 3.18 required registrars to maintain and publish contact details to receive reports of abuse, including Illegal Activity. This provision also outlined requirements relating to the investigation of and response to reports of abuse involving Registered Names sponsored by a registrar, and the related records a registrar must maintain. The requirements in RAA Section 3.18 have been amended as follows:

Commented [A3]: The proposed amendments focus on Section 3.18 -- which is an important section of the RAA in terms of DNS Abuse mitigation obligations. However, as noted in comments on the RAA, other sections of the RAA would benefit from amendments to further enhance DNS Abuse prevention/mitigation, such as registrant verification as noted above, among other aspects of the agreement. The BC believes these areas should be explored in future micro-PDPs or similar forums for ongoing community work.

Requirements Relating to the Publication and Maintenance of Abuse Contacts (RAA 3.18.1)

Where to Report Abuse[3]

To facilitate submission of reports from any party alleging abuse and/or Illegal Activity, the registrar must publish an email address or web form that is readily accessible on the homepage of the registrar's website[4]. Web forms must not require a login to submit abuse reports.

A registrar's homepage that clearly displays a link to a "Report Abuse'' or a "Contact Us" page (which clearly includes the abuse contact) and that allows reporters to easily submit reports from the linked page will be deemed compliant.

Confirmation of Receipt of a Report of Abuse

Additionally, the registrar must provide the abuse reporter with confirmation that the report has been received. This receipt confirmation may be sent to the abuse reporter or displayed on the screen upon completion of the submission to the registrar. This receipt confirmation must contain enough information for the reporter to be able to demonstrate that it submitted the abuse report. At a minimum, the receipt confirmation must identify the registrar, the reported Registered Name(s), and the date the report was submitted.

Contacts for Law Enforcement Agencies

The requirements related to contacts dedicated to receiving reports from Law Enforcement Agencies (LEA) and other authorities within the registrar's jurisdiction previously described in Section 3.18.2 of the RAA are now in RAA Section 3.18.3; these requirements remain unchanged.

Requirements Relating to Taking Mitigation Actions Upon Receipt of Actionable Reports of DNS Abuse (RAA 3.18.2)

Section 3.18.2 of the RAA, as modified by the DNS Abuse Amendments, now reads:

> *When Registrar has actionable evidence that a Registered Name sponsored by Registrar is being used for DNS Abuse, Registrar must promptly take the appropriate mitigation action(s) that are reasonably necessary to stop, or*

Commented [A4]: Please refer to comments regarding the introduction of the web form reporting option. If those proposed revisions cannot be introduced directly within the RAA, we would urge ICANN to include them in this Advisory -- i.e. that web forms do not impose unreasonable rate or size limits, allow file attachments, and permit other procedures that allow abuse reporting submissions to be complete and correct.

Commented [A5]: We would urge ICANN to require confirmations of reports be provided by email to the reporter, including a full copy of the report for record keeping and tracking purposes.

[3] For the avoidance of doubt, the requirements related to publishing the registrar's abuse contact email address and phone number through the Registration Data Directory Service (RDDS) remain unchanged.

[4] This website should be located at the same uniform resource locator (URL) that the registrar displays as the value for the "Registrar URL" field through its RDDS, provided to ICANN and to the registry operator for publishing in the registry operator's RDDS.

otherwise disrupt, the Registered Name from being used for DNS Abuse. Action(s) may vary depending on the circumstances, taking into account the cause and severity of the harm from the DNS Abuse and the possibility of associated collateral damage.

Actionable Evidence

The evidence must be *actionable*. This means that the information that is readily available to the registrar must be sufficient to enable the registrar to make a reasonable determination as to whether the Registered Name is being used or was being used for one or more forms of DNS Abuse. Registrars are encouraged to proactively monitor the Registered Names that they sponsor to identify potential DNS Abuse. A registrar's assessment of actionable evidence will vary depending on the circumstances of each case.

Obtaining Actionable Evidence From an External Party

The Contracted Parties House (CPH) published guidelines to assist with the submission of complete and actionable abuse reports to registrars (CPH Guidelines). The CPH Guidelines describe the evidence that tends to make an abuse report actionable. For example, a screenshot showing a phishing attempt with an indication of what the phish is against (a financial institution, for example); and the complete URL where the abuse is located (e.g., example[.]tld/badpage[.]html)[5]. Abuse reporters are encouraged to review and follow the CPH Guidelines, and to provide as much information as possible within their reports, to enable the registrar to conduct an investigation into potential DNS Abuse.

Commented [A6]: Comments from some registrars suggested that more information is not always helpful. The information submitted should be focused and relevant, and not extraneous. The Advisory could clarify this.

In instances where a registrar receives an abuse report that does not contain all necessary information to be considered actionable evidence of DNS Abuse, the registrar must still investigate per Section 3.18 of the RAA. In some cases, the registrar may have access to information that was not provided by an abuse reporter but is necessary or helpful to determine that the Registered Name is being used for DNS Abuse. In such cases, the registrar should consider information that it can reasonably access and is relevant to the investigation (e.g., name servers, account information and activity, and contents of at least the primary webpage or specific URL in the abuse report, if provided). If this information available to the registrar, combined with information provided in the external party's abuse report, is sufficiently actionable to enable the registrar to determine that an incident of DNS Abuse is occurring or has occurred, this is sufficient to trigger the registrar's obligations regarding mitigating such incident of DNS Abuse under Section 3.18 of the RAA.

After Actionable Evidence, Prompt Action Is Required

Upon obtaining actionable evidence, the registrar must *promptly* take *appropriate mitigation action(s)* that are reasonably necessary to stop, or otherwise disrupt, the

[5] This URL is shown in a format known as a "defanged URL." A defanged URL is readable to the human eye but not clickable. Therefore, if you or the recipient of your abuse report click on the URL by mistake, it will not direct you or the recipient to a potentially malicious site.

Registered Name from being used for DNS Abuse. To determine the mitigation actions that are prompt and appropriate, the registrar will consider the specific circumstances of the case, which may include balancing the scope and intensity of the harm caused by the DNS Abuse against the possibility of associated collateral damage.

Collateral damage is a particularly important consideration when an otherwise legitimate or benign domain name is used as a vector for DNS Abuse without the knowledge or consent of the registrant. This is often referred to as a "compromised domain" and sometimes is a result of an exploited website content management system. In these compromise situations, direct suspension of the domain by the registrar or registry operator may not be the appropriate mitigation, as suspension will cut off access to all legitimate content as well as render any associated email and other services with the domain inaccessible[6]. This is also the case when the DNS Abuse is associated with a third-level or subdomain. Registrars and registries can only act at the second-level domain level. Therefore, if they suspend the second-level domain, all third-level domains would be suspended as well, not just the one associated with DNS Abuse. In these situations, a registrar might elect to provide notification to the registrant, site operator, and/or web host. In circumstances where the registrar has determined that collateral damage resulting from the suspension of a second-level domain outweighs the benefit of mitigating or disrupting the reported DNS Abuse, the registrar should notify any relevant parties that would be in a position to mitigate or disrupt the DNS Abuse without causing such collateral damage and/or notify the reporter and identify which parties would be in such a position. The registrar should continue to serve as an escalation pathway in the event other parties in the ecosystem are unresponsive or unable to mitigate the abuse, and this factor should be taken into consideration by the registrar in reassessing potential collateral damage versus mitigation benefits.

What Makes an Action Prompt

As noted above, the appropriate mitigation action to stop or disrupt an instance of DNS Abuse will vary depending on the specific circumstances. Consequently, the appropriate amount of time to investigate and take action will also vary, making it impossible to prescribe a fixed amount of time for an action to be considered "prompt." Instead, registrars must demonstrate an ongoing attentiveness to allegations of sponsored names being used for DNS Abuse. The attentiveness should be commensurate with the potential harm that DNS Abuse causes victims.

Accordingly, in response to an inquiry by ICANN Contractual Compliance, registrars will be required to explain how the actions were prompt considering the specific circumstances. ICANN Contractual Compliance will then review the explanation and the relevant circumstances to make a case-by-case determination as to whether the actions were reasonably prompt. The timelines in the examples included in this Advisory are not contractual requirements, but illustrative only. A registrar taking more time to investigate and take action against a case similar to the examples will not necessarily be indicative of noncompliance. Conversely, other circumstances may require the registrar to act more quickly, such as instances of DNS Abuse that carry the potential of causing

Commented [A7]: Although we agree with the need for some flexibility on response timelines, there should be a responsiveness floor below which registrars are not permitted to go (i.e. responses/action within no more than 10 calendar days from the date a report was submitted).

[6] More information on collateral damage and proportionality considerations when acting at the DNS level is available in the Internet and Jurisdiction Policy Network's publication "Toolkit: DNS Level Action to Address Abuses."

imminent harm to end users. A registrar is expected to investigate and take action as soon as possible following the registrar's reasonable attempt to confirm an instance of DNS Abuse.

What Makes an Action Appropriate

A registrar is expected to investigate and take appropriate action that is reasonably necessary to mitigate or otherwise disrupt reported DNS Abuse. In general, the actions available to a registrar to meet this obligation, where DNS Abuse is confirmed and there is no concern with collateral damage, include: suspending the domain name(s) (i.e. placing the domain name(s) on clientHold status in EPP), cancelling the registration, or transferring the registration to a third party, as well as potentially applying a transfer lock to prevent the registrant from moving the domain to another registrar to resume abusive activities, and applying clientRenewProhibited EPP status to prevent the registration from renewing. Additional actions might include suspending or terminating a particular registrant's account with the registrar, identifying any other domain names that may be registered to the same registrant to determine if other domains under the registrar's management may also be in use in connection with DNS Abuse and similarly taking action regarding any such additional domain names, and/or conferring with other registrars and/or registry operators to determine if the registrant has engaged in DNS Abuse via other domain names managed through other registrars and collaborating to address the full scope of the DNS Abuse associated with a particular registrant.

Putting It All Together – Registrar Examples of Compliance

The examples below illustrate reasonable and prompt mitigation actions taken to stop the Registered Name from being used for DNS Abuse (Scenario One) and to disrupt the course of the DNS Abuse in relation to the Registered Name (Scenario Two). These scenarios contain specific factual circumstances. Under different circumstances, individual registrars may take different actions and within a different time frame to stop, or otherwise disrupt, individual cases of DNS Abuse. In all instances, registrars must be able to demonstrate that any approach taken is compliant with the ~~relevant~~ requirements in Section 3.18 of the RAA.

Scenario One: A registrar receives a complete and actionable abuse report alleging that a Registered Name sponsored by the registrar is used for phishing. The report includes evidence that a URL containing the Registered Name sponsored by the registrar is being sent via email or SMS representing itself as a large bank requesting the recipients unlock their accounts. The registrar initiates an investigation considering all relevant information included in the abuse report. The registrar's investigation reveals the Registered Name has no publicly available website and only displays a direct URL with what appears to be a login screen for a large bank. The same URL is the one being sent via emails or SMS. The registrar also considers that the customer is new and the Registered Name was registered five days prior.

Appropriate Mitigation Actions: The registrar reasonably concludes the Registered Name is being used for DNS Abuse and stops the DNS Abuse by suspending the Registered Name, applying the clientHold Extensible Provisioning Protocol (EPP) status code[7]. The investigation and mitigation action occur within two business days of receipt of the report of abuse. The registrar may also decide to apply a transfer lock to the Registered Name to prevent the registrant from attempting to evade the mitigation action and resume using the domain name for

DNS Abuse, so long as the registrar complies with the applicable requirements in ICANN's Transfer Policy.

Scenario Two: A registrar receives a complete and actionable abuse report alleging that a Registered Name sponsored by the registrar, autobrand.tld, is being used for phishing. The report of abuse includes evidence of a specific URL being used for phishing. The registrar investigates, considering all relevant information included in the abuse report as well as information readily and reasonably accessible to the registrar.

[7] Click here for more information from ICANN about EPP Status codes.

The investigation confirms that the URL in the report of abuse is being used for phishing. The investigation also reveals that the URL belongs to a subdomain (city.autobrand.tld), and appears to be used by a franchisee. The registrar acknowledges that the Registered Name autobrand.tld was registered three years ago and has a robust set of content for an automobile dealership franchise. The registrar is able to confirm the Registered Name is used for Autobrand's corporate emails and subdomains for multiple franchisees.

Appropriate Mitigation Actions: The registrar reasonably concludes that the Registered Name is being used for DNS Abuse, but that it is likely the result of domain compromise and that the registrant is not knowingly using the Registered Name for DNS Abuse. The registrar assesses the potential collateral damage that suspending the domain name would have, and reasonably concludes that is not an appropriate mitigation action at this time. Instead, the registrar disrupts the DNS Abuse by notifying Autobrand, the registrant of autobrand.tld, identifying the nature of the DNS Abuse and requesting that ~~it~~ Autobrand eliminate the phishing content by a certain date reasonably determined by the registrar. The investigation and mitigation action occur within three business days of the receipt of the abuse report.

Communicating Action to Reporters
Once reports are processed by the registrar, the registrar should provide an update via email to the reporter providing a brief summary of the actions taken and outcome, and a rationale for the actions taken (or if no action taken). In this update, if the registrar determined that no action on its part was appropriate, the registrar should identify other parties in the ecosystem to whom the reporter could direct the report who may be better situated to investigate and/or address the reported abuse.

Requirements Related to the Maintenance and Provision to ICANN of Records
The requirements related to documenting and providing records related to the receipt of and response to abuse reports previously described in Section 3.18.3 of the RAA are now in RAA Section 3.18.4; these requirements remain unchanged. These requirements also apply to the response to reports of DNS Abuse under Section 3.18.2.

Registry Operator Obligations

Section 4, Specification 6 of the RA

Specification 6, Section 4 of the RA requires the publication, and provision to ICANN, of contact details for handling inquiries related to malicious conduct in the top-level domain (TLD). It also includes requirements related to the removal of orphan glue records when used in connection with malicious conduct. The requirements in this Specification have been amended as follows:

Requirements Relating to the Publication and Maintenance of Abuse Contacts (Base RA Specification 6, Section 4.1)

Where to Report Abuse
To facilitate submission of reports from any party alleging malicious conduct in the TLD, including DNS Abuse, the registry operator must publish an email address or web form, a mailing address, and a primary contact for handling such reports.

A registry operator's homepage that clearly displays a link to a "Report Abuse" or a "Contact Us" page (which clearly includes the abuse contact) where submission of reports is unimpeded will be deemed compliant.

Confirmation of Receipt of a Report of Abuse
Upon receipt, the registry operator shall provide the abuse reporter with confirmation that the report has been received. This receipt confirmation may be sent to the abuse reporter or displayed on the screen upon completion of the submission to the registry operator. This receipt confirmation must contain enough information for the reporter to be able to demonstrate the submission of the abuse report. At a minimum, the receipt confirmation must identify the registry operator, the reported Registered Name(s), and the date on which the report was submitted.

Requirements Relating to Taking Mitigation Actions Upon Receipt of Actionable Reports of DNS Abuse (Base RA Specification 6, Section 4.2)

Section 4.2 of Specification 6, as modified by the DNS Abuse Amendments, now reads:

> *Where a Registry Operator reasonably determines, based on actionable evidence, that a registered domain name in the TLD is being used for DNS Abuse, Registry Operator must promptly take the appropriate mitigation action(s) that are reasonably necessary to contribute to stopping, or otherwise disrupting, the domain name from being used for DNS Abuse. Such action(s) shall, at a minimum, include: (i) the referral of the domains being used for DNS Abuse, along with relevant evidence, to the sponsoring registrar; or (ii) the taking of direct action by the Registry Operator, where the Registry Operator deems appropriate. Action(s) may vary depending on the circumstances of each case, taking into account the severity of the harm from the DNS Abuse and the possibility of associated collateral damage.*

Commented [A8]: Same comments as above regarding web form submission option.

Commented [A9]: Same comments as above regarding confirmations of receipt.

Actionable Evidence

The evidence must be *actionable*. This means that the information that is readily available to the registry operator must be sufficient to enable the registry operator to make a reasonable determination as to whether the Registered Name is being used or was being used for one or more forms of DNS Abuse. Registry operators may obtain actionable evidence by reviewing information that they can reasonably and independently access, whether in conjunction with a report of abuse or as part of their own efforts under Specification 11(3)(b) of the Registry Agreement by conducting technical analysis to identify domains being used for DNS Abuse. Actionable evidence can also be presented to the registry operator by an external party such as LEA, the relevant registry operator's trusted or recognized sources, or any other party or source. Abuse reporters are encouraged to provide as much information as possible to contribute to ensuring the registry operator has sufficient information to conduct an investigation into potential DNS Abuse. For the avoidance of doubt, an abuse report considered incomplete by the registry operator may still be deemed actionable if the registry operator has access to sufficient information to reasonably conduct an investigation to determine whether the reported Registered Name is used for DNS Abuse.

Commented [A10]: Same comments as above regarding amount of information provided. We also note that while registrars have provided guidance regarding kinds of information to make reports actionable, similar guidance should apply to registry operators as well (or other guidance provided where this may differ for any reason).

After Actionable Evidence, Prompt Action Is Required

Upon obtaining actionable evidence, the registry operator must promptly take appropriate mitigation action(s) that are reasonably necessary to contribute to stopping, or otherwise disrupting, the domain name from being used for DNS Abuse. To determine the appropriate actions, the registry operator will consider the specific circumstances of the case, which may include balancing the scope of the harm and victimization caused by the DNS Abuse against the possibility of associated collateral damage. The importance of collateral damage in the situation of compromised domains described above for registrars applies equally to registries.

The registry operator will also consider whether it, the sponsoring registrar, and/or another party are the best-equipped parties to review and take the appropriate, proportionate mitigation actions. For example, for a single Registered Name being used for DNS Abuse, the registrar may be best placed to review and address the DNS Abuse with its customer. Similarly, in the case of compromised systems, the Registered Name Holder or the hosting provider that maintains administrative access to affected systems may be better able to address the issues, and the registry operator should refer these to the registrar first, as suspending the domain by applying either clientHold or serverHold can cause collateral damage on benign or legitimate content. On the other hand, the registry operator may be the best party to address large-scale threats that span many Registered Name Holders or registrars, such as domain-generating algorithms used to propagate botnets, or in cases where the registrar or other parties in the ecosystem are unresponsive or otherwise do not act to mitigate or disrupt the identified DNS Abuse.

The mitigation actions promptly taken must be reasonably necessary to ~~achieve one of the following outcomes: *contributing to* *stopping*~~ or *disrupting* the ~~Registered Name from being used for~~ DNS Abuse. At a minimum, the registry operator must:

1) *Report* the Registered Name(s) and *supply* the relevant evidence to the sponsoring Registrar(s); or
2) *Take direct action* on the Registered Name(s) where the registry operator deems such direct action appropriate.

What Makes an Action Prompt

As noted above for registrars, the appropriate action to take to mitigate or disrupt an instance of DNS Abuse will vary depending on the specific circumstances.
Consequently, the appropriate amount of time to investigate and take appropriate action will also vary, making it impossible to prescribe a fixed amount of time for an action to be considered "prompt." Instead, registry operators must demonstrate an ongoing attentiveness to allegations of sponsored names being used for DNS Abuse. The attentiveness should be commensurate with the potential harm DNS Abuse causes victims.

Commented [A11]: Same comments as above regarding promptness (i.e. a floor should be set for timeline for response, i.e. no more than 10 calendar days).

Accordingly, in response to an inquiry by ICANN Contractual Compliance, a registry operator will be required to explain how the actions were prompt considering the specific circumstances. ICANN Contractual Compliance will then review the explanation and the relevant circumstances to make a case-by-case determination as to whether the actions were prompt. The timelines in the examples included in this Advisory are not contractual requirements, but illustrative only. A registry operator taking more time on a particular case will not necessarily be indicative of noncompliance. Conversely, other circumstances may require the registry operator to act more quickly, such as instances of large-scale threats that carry the potential of causing imminent harm to a large number of end users. A registry operator is expected to investigate and take action as soon as possible following the registry operator's reasonable attempt to confirm an instance of DNS Abuse.

The examples below illustrate reasonable mitigation actions promptly taken to contribute to stopping the Registered Name from being used for DNS Abuse (Scenario Two) and to contribute to disrupting the course of the DNS Abuse in relation to the Registered Name (Scenarios One and Three). These scenarios contain specific factual circumstances. Under different circumstances, individual registry operators may take different actions with different time durations to contribute to stopping, or otherwise disrupting, individual cases of DNS Abuse. In all instances, registry operators must be able to demonstrate that any approach taken is compliant with the relevant requirements in Section 4.2 of Specification 6 of the RA.

Section 3(b), Specification 11 of the RA
This section was modified to substitute the defined term of DNS Abuse as set forth in the amendments to Specification 6, Section 4, for "security threats."

What Makes an Action Appropriate

A registry operator is expected to investigate and take appropriate action that is reasonably necessary to mitigate or otherwise disrupt reported DNS Abuse. In general, a registry operator may choose to redirect a report to the registrar to action directly. However, in circumstances where the registry opts to act directly in the first instance, the actions available to a registry operator to meet this obligation, where DNS Abuse is confirmed and there is no concern with collateral damage, include: suspending the domain name(s) (i.e. placing the domain name(s) on serverHold or inactive status in EPP), cancelling the registration, or transferring the registration to a third party, and/or applying serverRenewProhibited EPP status to prevent the registration from renewing. Additional actions might include identifying any other domain names that may be registered to the same registrant to determine if other related domains within the registry zone may also be in use in connection with DNS Abuse and similarly taking action regarding any such additional domain names, and/or conferring with other registrars and/or registry operators to determine if the registrant has engaged in DNS Abuse via other domain names managed through other registrars and collaborating to address the full scope of the DNS Abuse associated with a particular registrant. In addition, where the registry operator has directed an abuse report to the registrar, but the registrar is unresponsive or unable or unwilling to properly address the abuse, the registry should act as an escalation pathway and resume responsibility for taking mitigation or disruption action directly.

Putting It All Together – Registry Operators Examples of Compliance

Scenario One: A registry operator received a notification from a credit union (Example Credit Union) via its abuse webform that someone registered the domain <loginexamplecreditunion[.]TLD> six days ago and the credit union alleges the domain is engaged in phishing. The credit union provides a screenshot showing a webpage on the domain gathering login credentials.

Appropriate Mitigation Actions: Following its internal process, the report is processed and reviewed by the registry operator within two business days. Upon concluding its investigation, the registry operator reasonably determined that the Registered Name was being used for DNS Abuse. Therefore, the registry operator disrupts the course of the DNS Abuse by notifying and providing all pertinent information to the sponsoring registrar. The registry operator includes a time-bound request for the registrar to investigate and take the reasonably necessary mitigation actions to stop, or otherwise disrupt, the DNS Abuse. By the given deadline, the registry operator is able to confirm that the registrar suspended the Registered Name via applying the clientHold EPP status code.

Scenario Two: A registry operator is approached by LEA and provided evidence that a series of domains are, or will be, involved in a domain-generating algorithm associated with a botnet. The botnet involves some existing Registered Names, but predominantly domains that are not yet registered.

Appropriate Mitigation Actions: Within six hours of concluding its investigation and reasonably confirming the DNS Abuse, the registry operator contributes to stopping the DNS Abuse by taking actions as directed by or agreed upon with the LEA. In this case, the registry operator has agreed that for the relevant Registered Names, the registry will delegate to different name server(s) (e.g., redirect the name servers or sinkhole) at the request of LEA. The registry operator also directly creates the domains for those previously the unregistered domains associated with the botnet as requested by LEA. Noting that domain creation by the registry operator ordinarily requires permission via ICANN's Security Response Waiver (SRW)[8]. The registry operator also will make a timely request to obtain a contractual waiver. It is noted, however, that an SRW may also be applied for as soon as is reasonably practicable after the fact, and ICANN org may respond with a retroactive waiver if appropriate, so as to not delay the support of the LEA operation[9].

Scenario Three: As part of its technical analysis looking for DNS Abuse under Specification 11(3)(b), a registry operator discovers that a subpage of a domain is being used to distribute malware while the remainder of the site on the domain appears to be legitimate or benign content. The domain name has been registered for three years.

Appropriate Mitigation Action: Within three hours of determining that the Registered Name is being used for DNS Abuse and compromised, the registry operator contributes to disrupting the course of the DNS Abuse by notifying and providing all pertinent information to the sponsoring registrar and making a time-bound request for action by the registrar to report back. The registrar then notifies the registrant directly, which resolves the issue by updating its content management system to remove the malware.

[8] Information about Security Response Waivers can be found on this page.

Scenario Four: A registry operator received a notification from a credit union (Example Credit Union) via its abuse webform that someone registered the domain <loginexamplecreditunion[.]TLD> six days ago and the credit union alleges the domain is engaged in phishing. The credit union provides a screenshot showing a webpage on the domain gathering login credentials.

Appropriate Mitigation Actions: Following its internal process, the report is processed and reviewed by the registry operator within two business days. Upon concluding its investigation, the registry operator reasonably determined that the Registered Name was being used for DNS Abuse. Therefore, the registry operator disrupts the course of the DNS Abuse by notifying and providing all pertinent information to the sponsoring registrar. The registry operator includes a time-bound request for the registrar to investigate and take the reasonably necessary mitigation actions to stop, or otherwise disrupt, the DNS Abuse. In the event the registrar is unresponsive and fails to take further action by the registry operator's stated deadline, the registry operator resumes responsibility for mitigating the confirmed DNS Abuse by placing the domain name into serverHold status in EPP. The registry should follow-up with ICANN Compliance, the registrar, and the original abuse reporter, as appropriate, to determine why the registrar failed to act on the registry operator's request. This follow-up by the registry enables the registrar and original abuse reporter to improve their processes for future requests.

Communicating Action to Reporters
Once reports are processed by the registry operator, the registry operator should provide an update via email to the reporter providing a brief summary of the actions taken and outcome, and a rationale for the actions taken (or if no action taken). In this update, if the registry operator determined that no action on its part was appropriate, the registrar should identify other parties in the ecosystem to whom the reporter could direct the report who may be better situated to investigate and/or address the reported abuse.

ICANN Org's Investigations Into Compliance With the New Section 3.18.2 of the RAA and Section 4.2 of Specification 6 of the RA

What Would Constitute a Complete, Well-Evidenced, and Compliant Response? ICANN Contractual Compliance will enforce the requirements explained in this Advisory through the processing of external complaints, proactive monitoring, and audit activities. When ICANN Contractual Compliance receives a complaint, it will review any evidence submitted by the reporter as well as any available relevant information to determine whether a compliance case must be initiated with the relevant registrar or registry operator. In the absence of sufficient evidence in support of a claim of DNS Abuse, ICANN Contractual Compliance will close the case as invalid. Among other things, this review will consider whether information readily available to the sponsoring registrar directly or through a reseller, or the registry operator, as applicable, is sufficient to reasonably determine that the Registered Name is being used for one or more forms of DNS Abuse. The review will also consider if there was any additional information provided by the reporting party in response to the registrar's or registry operator's requests for additional information or evidence.

Furthermore, where applicable and relevant to the specific case, ICANN Contractual Compliance will: (1) review relevant, publicly accessible data displayed through the Registration Data Directory Service, e.g., creation date, EPP status(es), or name servers information; and (2) perform DNS lookups to determine whether the reported Registered Names resolve in the DNS. ICANN Contractual Compliance may also conduct its own research and review additional, relevant information on a particular Registered Name alleged to be involved in DNS Abuse.

When initiating a compliance case with a registrar or registry operator under Section 3.18.2 of the RAA or Section 4.2 of Specification 6 of the RA, respectively, ICANN Contractual Compliance will provide an itemized list of all the information and records needed to assess compliance as it pertains to the reported Registered Names(s) and forms of the alleged DNS Abuse. In response to a compliance case, the registrar and registry operator will be expected, at a minimum, to:

- Explain how and why the registrar or registry operator reached the determination that the evidence obtained was not actionable, where applicable. For example, a registrar may explain that, after reviewing the information and records submitted by the reporting party, and through its investigation, the registrar was not able to verify that the DNS Abuse was taking place in connection with the reported Registered Name(s). ICANN Contractual Compliance may ask the registrar or registry operator to clarify any clear discrepancies between the explanation given and any information and data captured by ICANN Contractual Compliance during the complaint validation process.
- Provide a detailed explanation, supported by the relevant records, of the specific mitigating actions taken, when the actions were taken, and how the actions taken were considered prompt and reasonably necessary to stop or to disrupt or to contribute to stopping or disrupting, as it pertains to the specific circumstances of the case (including any applicable explanation relating to disproportionality of actions at the DNS level and collateral damage). The requirements for the registrar to provide this information will continue to apply in cases in which the registrar elects to delegate the investigation of the DNS Abuse report to a reseller. In such cases, the registrar retains the obligation to demonstrate compliance with Section 3.18 of the RAA[10] by explaining the actions it took as well as those actions of any other delegated parties such as resellers and providing related records.

[9] For more information on how registries can work with law enforcement and ICANN to address domain- generating algorithms, please see "Framework on Domain Generating Algorithms Associated With Malware and Botnets," published by the Government Advisory Committee Public Safety Working Group and the gTLD Registries Stakeholder Group.

[10] See Section 3.12 of the RAA.