DNA HEALTHY DOMAINS INITIATIVE REGISTRY / REGISTRAR HEALTHY PRACTICES

I. Introduction and Context

Introduction

This document is part of the Domain Name Association's (DNA) Healthy Domains Initiative (HDI), which has the following objectives:

- Establish a network of industry partners that communicate and collaborate with one another to support a healthy domain name ecosystem.
- Identify and/or develop industry-accepted healthy practices and specific programs that provide tangible ways of promoting standards for healthy domains.
- Demonstrate to the community our desire to implement best practices and otherwise fulfill our stewardship obligations

Purpose of this Healthy Practices Document

The purpose of this document is to present a set of prioritized healthy practices and programs for the domain name community that would result in:

- Presentation of a more vibrant namespace to end-users
- Identification of additional voluntary steps to address abuse and illegal activity

The document is meant to be collaborative among all interested parties. It is anticipated that this set of draft principles and operational programs will continually evolve.

This document is not meant to create new requirements for registries and registrars; it is a representation of existing and proposed practices that, voluntarily adopted, can further the healthy development of the domain name system.

Context: Evolution of Healthy Domains Initiative

The Healthy Domains Initiative is a project under the DNA's umbrella. The DNA assumed management of the concept in 2015 and established a committee devoted to HDI.

As the concept took shape, the HDI committee entertained ideas for registry and registrar operations that, if implemented, would help to address various challenges in the domain name system. Such ideas were presented and discussed by multiple parties in the greater community at the initiative's first HDI summit, held in Seattle in February 2016. The Seattle meeting further built out these ambitious ideas.

During the ICANN meeting in Marrakech in March 2016, parties interested in HDI met to further review and discuss these ideas. It was agreed in that meeting that the next best output for the HDI effort was to put forth a set of operational principles to which contracted parties could reasonably adhere. HDI leaders thus focused on such a document as the first deliverable in the HDI effort.

Next, to get a sense of what already was in place in the market, and to measure priorities for potential practices, the DNA conducted a survey of members—the results of the survey identified areas where contracted parties already had put strong operational practices into place, and where there was

room for additional expansion. The results of that survey are below in this paper, embodied as a prioritized list of aspirational practices.

After conferring on these proposals during the ICANN meeting in Helsinki in June 2016, the HDI committee identified several that should be prioritized, developed and implemented. These are:

1. Addressing online security abuse (e.g., malware, phishing, pharming)
2. Enhancing child abuse mitigation systems
3. Complaint handling from illegal or "rogue" online pharmacies

Baseline: Industry Respondents Detail Current Healthy Practices

The DNA surveyed its membership on what, if any, healthy practices already are employed by contracted parties, and further, regarding the appeal of proposed new practices.

An impressive 78% of respondents said that their companies already employed healthy practices outside the scope of their contracts with ICANN.

89% of respondents said they intend to expand this list to include additional practices. The conclusion of the survey, agreed to by most involved in HDI, is that there exists an opportunity to expand practice ideas, and contracted parties are receptive to doing so.

II. Healthy Practice Priority Areas

A. Addressing online security abuse (e.g., malware, phishing, pharming)

For a full review of proposed healthy practices addressing this area, please see the sub-team's detailed document in Appendix A.

Overview
The objective of this effort is to further reduce security abuse in the DNS.

Tactics and goals
This effort will consolidate recommended practices for registries and registrars responding to security abuses identified in their TLDs described in past work by groups in the security space. In identifying recommended practices, we consulted past practices recommendations developed by the Security and Stability Advisory Committee (SSAC); Anti-Phishing Working Group (APWG); Stop Badware; the Messaging, Malware, and Mobile Anti-Abuse Working Group (M3AAWG) as they applied to the registry and registrar context. Our goals in this area are threefold:

- To outline some of the challenges and considerations affecting how registries and registrars respond to identified security threats;
- To identify of practices for registries and registrars to improve responses to security threats through individual practice, collective action, and information sharing; and
- To identify a means for registries and registrars to strengthen their relationships with key groups in the security space to improve and evolve security-related abuse handling.

Relevant principles

Principle 1: Focus action on domains that are primarily malicious.

Principle 2: Consider the impact of mitigation mechanisms, particularly on third parties, and whether another provider is able to mitigate the abuse through narrower, less disruptive means.

Recommended practices

This sub-group has identified a total of 20 practices for registrars and registries to employ as means for combating DNS abuse. The specific recommendations are consolidated around four core areas where registries and registrars can exercise strong security practices:

- Measures to improve credential management on their platforms and minimize the risks associated with compromised domains;
- Measures to detect and mitigate possible abuse at the point of registration;
- Measures to identify and mitigate potential abuse on an ongoing basis; and
- Measures for receiving and handling abuse reports.

We do not intend to propose a one-size-fits-all model for security abuse handling. The ideal package of security improvements may depend on registrar's customer base and business model. Specific considerations and recommendations for each of these four areas are identified in Appendix A.

B. Enhancing child abuse mitigation systems

For a full review of proposed healthy practices addressing this area, please see the sub-team's detailed document in Appendix B.

Overview

The objective of this practice is to further expand existing—but not yet universal—methods for addressing images and content related to child abuse, as well as, providing education and resources for registries and registrars to combat child abuse.

Tactics and goals

The primary recommended practices here are twofold:

- Establish a system for imagery handling
    - Participating registry operators and registrars require in their registry –registrar agreements/registrant agreement a term that prohibits child abuse content and permits the registry operator/registrar to suspend or delete domain names that violate this term.
    - Each also may establish an internal policy/protocol advising staff to forward the URL/domain name/website in question to the organization's Legal or Compliance Department.
    - The next step is an expeditious report of the situation to a child protection hotline.
- Establish a trusted notifier system
    - "Trusted notifier" is a party that is pre-vetted (e.g., NCMEC, IWF, INHOPE) and recognized by the contracted party as capable of providing the relevant and complete evidence needed to take action against the registrant.
    - Provide forms of agreements between registries/registrars and these organizations.

Aspirational practices

Depending on the services provided, contracted parties may also wish to consider adoption of services and technologies available through outside child protection expert organizations. These include:

- NCMEC's URL Initiative and Photo DNA and Hash Value Sharing programs
- IWF's Image Hash Tag List

C. Complaint handling for "rogue" online pharmacies

For a full review of proposed healthy practices addressing this rogue pharma, please see the sub-team's detailed document in Appendix C, and NABP's diagram proposal for a qualified complaint handling system in Appendix E.

Overview

The objective of this practice is to further address "rogue," or illegal online pharmacies.

Tactics and goals

The proposed methods for this section of HDI's healthy practices proposal involves both internal and external steps that registries and registrars may voluntarily employ to identify and safely remove these threats to public health:

- Internal practices by contracted parties:
    - Partner with and support the work of organizations dedicated to combating the problem (NABP, CSIP, ASOP).
    - Notify relevant organizations when the registry/registrar becomes aware of potential illegal pharmacies.
    - Take action on confirmed illegal pharmacy sites in accordance with internal processes.
- Establish a trusted notifier and third-party validation system
    - "Trusted notifier" is a party that is pre-vetted and recognized by the contracted party as capable of providing the relevant and complete evidence needed to take action against the registrant.
    - "Validator" is a party that the contracted party deems capable of determining that an online drug seller is properly licensed, reputable and safe.
    - Provide forms of agreements between registries/registrars and these organizations.

The DNA's role is to promote the use of sound internal practices and relevant partnerships to help mitigate the problem of illegal internet pharmacies.

III. Next Steps

In order to make measurable progress toward the above prioritized practices and therefore validate and claim ongoing success with the program, the DNA must now move into implementation mode. This includes the following steps:

1. Meet monthly as an HDI committee to continue progress toward implementation of prioritized practices.
2. Set interim progress report to full DNA organization between Hyderabad and Copenhagen
3. Prepare short PR campaign to alert industry to DNA efforts.

Appendix A: Security Threat Mitigation Proposal

Purpose

The purpose of this document is to consolidate recommended practices for registries and registrars responding to security abuses identified in their TLDs described in past work by groups in the security space. In identifying recommended practices, we consulted past best practices recommendations developed by the Security and Stability Advisory Committee (SSAC); Anti-Phishing Working Group (APWG); StopBadware; and the Messaging, Malware, and Mobile Anti-Abuse Working Group as they applied to the registry and registrar context. Our goals in this area are threefold:

- To outline some of the challenges and considerations affecting how registries and registrars respond to identified security threats;
- To identify of practices for registries and registrars to improve responses to security threats through individual practice, collective action, and information sharing; and
- To identify a means for registries and registrars to strengthen their relationships with key groups in the security space to improve and evolve security-related abuse handling.

Considerations

Several considerations complicate registries and registrars' efforts to effectively deal with online security abuse. Abuse complaints may invoke distributed actors and complex chains of responsibility. Various actors including registries, registrars, resellers, hosting providers, each have distinct responsibilities with respect to a domain name or website and different information and tools to assist in mitigating a particular abuse. The lack of uniform reporting and response practices across these providers may thwart the communication and collaboration necessary to effectively address a particular abuse. Further, given this distribution of service providers associated with a single domain name or website, a particular provider may lack a contractual relationship and/or history of communication with the registrant or site owner, limiting their ability to work directly with the registrant or site owner to mitigate the abuse.

Additional legal considerations also inform registries and registrars' ability to respond to abuse, these considerations can range from concerns around whether a particular action could negatively impact free speech or raise privacy concerns, to jurisdictional issues, where multiple service providers involved are subject to different legal frameworks with different requirements and limitations affecting how they take action on an identified abuse.

Lastly, accountability considerations also factor significantly into registries and registrars' practices for handling identified security abuse. Most notably, the question of whether the registrant is directly responsible for the abuse in question should influence what actions a registry or registrar takes when a potential security abuse is identified. Domain names that appear to be compromised may require a different set of responses, given that registrants on the whole are generally uneducated about security threats without support from their providers.

These considerations have been taken to account in the principles and recommendations outlined below. However, they may account for additional differences in how particular registries or registrars address abuse complaints, or in how particular complaints are dealt with on a case-by-case basis.

Principles

Principle 1: Focus action on domains that are primarily malicious.

Registries and registrars should focus on domain names that are primarily malicious. Domains that are compromised or where other parts of the domain serve a legitimate purpose should generally be referred to their hosting providers, which possess tools to address abuse in a more targeted fashion by taking action against specific abusive content versus taking action at the domain level.

Principle 2: Consider the impact of mitigation mechanisms, particularly on third parties, and whether another provider is able to mitigate the abuse through narrower, less disruptive means.

Considerations that a registry or registrar could weigh when assessing whether they are appropriately situated to mitigate the identified abuse include:

- Whether the relevant infrastructure is under its direct control;
- The number of downstream providers that would be affected;
- Applications or legitimate content that could be affected by mitigating the abuse directly;
- Whether mechanisms exist to temporarily mitigate the abuse, and any potential consequences of temporary mitigation;
- Whether downstream providers have been contacted already and whether they have been responsive when contacted; and
- Whether the provider in question possesses a direct contractual relationship with the registrant.

Registries and registrars may consider whether there are downstream providers with closer relationships to the registrant and the content in question (e.g. contractual relationships or more targeted tools to target the abuse). If so, it may be more appropriate to refer the complaint to a downstream provider. If downstream providers have already been engaged, any actions taken so far should be taken into account in determining any future response.

Recommended Practices

The following recommendations offer ways for registries and registrars to improve their security offerings. We do not expect that registries or registrars will implement all of the mechanisms described below; rather, that the recommended practices will provide a framework to review current practices against and identify potential improvements.

We break out recommended practices into four categories based upon the phase of the registration or abuse response in which they occur:

- Measures to improve credential management and minimize the risk associated with compromised domains;
- Measures to detect and mitigate possible abuses at the point of registration;
- Measures to identify and mitigate potential abuse on an ongoing basis; and
- Measures for receiving and handling abuse reports.

Implementation of each of the following mechanisms can occur in a manner that takes into account the considerations outlined above.

Additionally, the ideal package of security improvements may be affected by a registrar's customer base and business model. By way of example, a corporate registrar that manages high-value and

highly-trafficked domain names may benefit from implementing heightened opt-in security features to enable registrants to take additional steps to protect their domains from being compromised. On the other extreme, registrars or registries that sell high volumes of low-cost domains may see more impact from mechanisms that prevent abuse at the point of registration or that automate, expedite, or scale abuse response procedures.

Measures to improve credential management and minimize the risk associated with compromised domains

As outlined above, one of the most critical considerations in determining how to respond to a particular security threat is whether or not the domain name is malicious or compromised. Cybercriminals benefit from taking control of legitimate websites versus registering malicious domains, as they are more likely to retain traffic, invoke consumer trust, and are less likely to be blocked by security software or flagged by reputation service providers (Compromised Websites, A User Perspective).

According to regular studies carried out by the APWG, the vast majority of domain names that are flagged for phishing are the result of domain compromise versus malicious registrations by phishers (APWG, Global Phishing Survey).[1] Compromised websites can also be linked to other forms of abuse, such the distribution of malware, including through "domain shadowing" where abusive third-level domains are set up under a legitimate second level domain name, potentially bypassing internal monitoring (SAC074, SSAC Advisory on Registrant Protection). This makes the implementation of mechanisms to prevent credential compromise at the registrant, registrar, and registry level a useful proactive step to preventing many security abuses.

Previous work by the SSAC has offered a number of proactive measures that registrars can implement to allow registrants to minimize the risks that their domains will be compromised, which have been summarized below:[2]

- ***Recommendation 1:*** *Registrars may make registrant accounts secure through credential design, such as heightened requirements for password length and complexity, encouraging or requiring registrants to rotate passwords, and preventing password reuse.*
- ***Recommendation 2:*** *Registrars may offer to registrants additional, opt-in features to make their accounts more secure. Examples include enabling two-factor authentication, offering tiered levels of access for different account roles, delivering notification of account changes to multiple contacts, introducing security questions or other challenge systems, using IP whitelisting, or creating per-domain access controls.*
- ***Recommendation 3****: Registrars may validate change requests to a domain name through secondary means and not use an email address associated with the domain in question to validate which may itself be compromised.*

Additionally, the advisories propose mechanisms that registries or registrars can implement to minimize the risk of compromise of registry or registrar authoritative systems.

---

[1] According to the three most recent Global Phishing Surveys carried out by the APWG for the domain names that were registered maliciously accounted for only 28.6 percent of malicious registrations. The rest are a result of compromised domains. (APWG, Global Phishing Survey: Trends and Domain Name Use in 2H2014 and 1H2015)

[2] The full recommendations by the SSAC on this matter can be found in SAC040 and SAC074.

- ***Recommendation 4****: Registries and registrars can structure internal processes to ensure that credentials are not stored in places where the might be compromised (e.g. internal bug logs, wikis, or tickets).*
- ***Recommendation 5****: Registries and registrars can maintain good practices for the storage and transmission of credentials including transmission of credentials over secure channels, storing protected versions of credentials, storing backups offline, and destroying records of credentials where they are no longer needed.*
- ***Recommendation 6****: Registries and registrars may implement clear practices to ensure that credentials are revoked and rotated when personnel with access to the information depart the organization.*
- ***Recommendation 7:*** *If a breach occurs, registries and registrars can notify registrants in a way that can be easily recognized and verified.*

Measures to detect possible abuses at the point of registration or inbound transfer

Registries and registrars can also implement mechanisms to identify and address possible security abuses at the point of registration. These mechanisms are particularly useful for registries or registrars that offer free or extremely low-cost domains, which have historically attracted abuse, and as a deterrent for abuse types that require the registration of large volumes of domains.

- ***Recommendation 8:*** *Registrars can prevent against automated registrations by screening for and limiting or investigating high registration volumes coming from a single account, or by implementing a CAPTCHA to help ensure that domains are being registered by a human.*
- ***Recommendation 9****: Registrars screen registrations for frequently abused terms; require additional identity verification information from registrants of these domain names. Flag domains for further review or require additional information or validation from the registrant prior to registration.*
- ***Recommendation 10****: Registrars validate payment information based on Payment Card Industry (PCI) Security Standards.*

Measures to identify and mitigate potential abuse on an ongoing basis

In addition to responding to security abuses that are identified and reported to a registry or registrar by third parties, registries and registrars can improve abuse handling by proactively identifying potential abuses and taking further mitigation action based on the type and severity of the abuse.

Registries and registrars can improve security by building an abuse program that identifies, investigates and actions abuse in their namespaces proactively, through partnership with reputation service providers or third-party "blocklist", rather than solely taking action in response to abuse complaints.

Registries are already required per their Registry Agreements to "periodically conduct a technical analysis to assess whether domains in the TLD are being used to perpetrate security threats, such as pharming, phishing, malware, and botnets." However, many registries remain uncertain or tentative in responding to security abuse identified through these means, given that they are far removed in the chain of responsibility discussed earlier and lack a contractual relationship with the registrant. Registries can improve the effectiveness of these technical analyses by defining clear practices for how to process and take action on abuses identified through technical analysis.

Registries and registrars that use a reputation service provider or third party blocklist should understand that provider's framework for classifying abuse types (e.g. phishing, malware, or social engineering ads); any indicators provided for determining whether a domain name is likely to be

malicious or compromised; and where an abuse has been identified (e.g. whether it is at the domain level or confined to a particular subdomain or subdirectory). Each registry or registrar can define an internal framework for how to take action on identified abuses that takes into account these factions and the classification schema used by their reputation service provider.

- ***Recommendation 11****: Registries and Registrars may work with reputation service providers to proactively identify domains that have been identified as abusive, classify/investigate them, and take action as appropriate.*

Unlike new domain registrations, which are unlikely to have a prior abuse history, domains being transferred into a new registrar may already appear on a third party blocklist. Registrars could prevent abuse within their domains under management by screening inbound transfers that have been flagged by their reputation service provider or by third party blocklists, and barring these transfers unless and until the registrant works with the respective provider(s) to have the domain delisted.

- ***Recommendation 12:*** *Registrars may screen domain names being transferred in for appearance on malware/phishing block lists and require that domain names are de-listed before they can be transferred in.*

The limitations on direct intervention by the registry when abuse is identified through its required technical analysis also creates an opportunity for registrars to improve security response practices either through implementation of a consistent framework for responding to reports that are passed down from the registry, or even by engaging similar service providers directly. Overall efforts to mitigate security threats would benefit from some coordination and shared expectation regarding how information would be relayed from registries to registrars (or other third party providers) for action, as well as, strong communication between registries and registrars and other engaged parties. This begins with the provision of meaningful abuse reports.

- ***Recommendation 13:*** *Where identified domain names are being referred to a third party for action, registries and registrars should include all available information about the identified abuse.*

Relevant information can include at minimum:

- The URL being reported;
- The date and time that the abuse was reported;
- The IP address when last reported;
- Other targets that the abuse is being reported to; and
- Contact information necessary for follow up.

The following information is optional but can be provided to the extent that it is available:

- Conditions necessary to reproduce the identified abuse;
- The scope of abusive behavior (e.g. whether it applies to a particular page, subdomain, or across the domain);
- How the abuse was identified;
- Any specific malicious code or executables that were identified;
- Any related URLs; and

- Any actions taken to date in response to the abuse complaint[3]

Additionally, a registry or registrar should be clear about what, if any, action it expects the third party to take with regard to the abuse; a time frame for the party to take the action and/or provide a response; and any escalation procedures that may be followed if no action is taken or no response is received.

Measures for receiving, handling, and taking action in response to abuse reports

Lastly, abuse can also be identified by a registry or registrar due to the receipt of a third party abuse report. As a first step, registries and registrars can define clear process flows for how these reports will be received and processed, and what standards and procedures will be followed to determine the appropriate course of action. All reports could undergo initial evaluation on a timely basis that establishes (1) whether the reported abuse is credible or can be confirmed; (2) whether the domain name being reported is primarily malicious; and (3) and whether the reported abuse is within the scope of control of the registry or registrar, or whether it should be referred to a third party.

- ***Recommendation 14:*** *Registries and registrars identify clear processes, criteria, and allocation of responsibilities for the takedown of clear-cut phishing sites, and escalation processes for reviewing other reports.*

The investigation should not focus solely on the domain(s) referenced in the report. Wider investigation can be used to identify and, potentially, take action on additional domain names that are also abusive. This may be the result of a wider account compromise or a malicious user.

- ***Recommendation 15:*** *When an abuse report is received and verified as abusive/malicious, registrars may review other domain names in the same user account or using the same credit card information.*

Just as the provision of complete reports between providers can help improve overall security responses, the provision of incomplete reports by third parties can get in the way of effective handling by the party receiving the abuse report. Often, registries and registrars receive reports that contain insufficient information to be actionable, or that do not describe prior or parallel actions being taken with respect to the particular abuse. Incomplete reports may require registries and registrants to engage in back and forth with the reporter before the abuse can be classified and flagged for action in accordance with its internal processes. Registries and registrars can help expedite this process by providing information and tools for reporters to provide meaningful and actionable reports on the first attempt. This could include help center or reference articles about what information a registry or registrar expects to receive in an abuse report, or web forms that identify mandatory and recommended fields facilitating the submission process. Relative consistency in terms of what information is expected across registries and registrars will also help and encourage third parties to provide actionable reports regardless of provider.

---

[3] Stop Badware's Reporting Practices for Badware URLs provides a sample abuse notification that contains the recommended elements.

- ***Recommendation 16:*** *Registries and registrars can provide tools and information to help Internet users provide meaningful abuse reports.*

Registries and registrars should also maintain a clear channel of communication with the reporter. This can be used to provide and receive additional information that may assist in mitigating the abuse. Additionally, it will increase reporters' confidence that their reports are being given due consideration, even in instances where the provider is unable to undertake direct action.

- ***Recommendation 17****: Registries and registrars notify a complainant as soon as their reporter is received and provide a mechanism for them to provide further information or communication related to the complaint.*
- ***Recommendation 18:*** *Registries and registrars provide additional notification when the reporter case is closed, including a description of any action taken.*

  If a registry or registrar believes that an abuse complaint is credible but not within its scope of action it may provide additional assistance to the registrant by passing on the report to a downstream provider (e.g. registry to registrar, registrar to hosting provider or reseller) directly or providing guidance to the registrant about how to identify and contact the downstream provider.

- ***Recommendation 19****: If a registry or registrar believes that a third party is better situated to mitigate a reported abuse, assist the reporter by identifying the appropriate provider to receive the report or by passing on the report directly.*

Where a domain name appears to be abusive, a registry or registrar can additionally provide assistance by notifying the provider and encouraging him or her to mitigate the abuse directly. To the extent practical, the registry or registrar can provide additional information or resources to assist the registrant in mitigating the abuse.

- ***Recommendation 20:*** *When a domain name appears to be compromised, a registrar may notify the registrant and provide an opportunity to rectify the abuse. Registries may, instead, notify the registrar and request that they or their reseller pass on the notice to the registrant.*

Appendix B: Child Abuse Content Mitigation Proposal

Different countries define child abuse images and child pornography differently (e.g., some deem computer-generated images/anime to be illegal whereas others do not). One global definition of "child abuse images" is the United Nations Convention on the Rights of the Child, which defines the term as any photograph, film, video, picture, or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, depicting child sexual abuse.

For more information about various global laws related to child protection, see:

www.icmec.org/wp-content/uploads/2016/02/Child-Pornongraphy-Model-Law-8th-Ed-Final-linked.pdf and http://fosigrid.org

Recommended practices for Registries and Registrars:

- ***Recommendation 1:*** Each Registry Operator / Registrar may publish, on their respective websites, a "zero tolerance" statement or policy against child abuse content and include specific provisions in their registration terms and conditions prohibiting child abuse content. Each Registry Operator/Registry may include the right to suspend or delete domain names that violate this term in their agreement.

  Sample Clause:

  Registrant's sites shall not display any child abuse images. Registrant's sites shall not engage in practices that are designed to suggest the presence of child abuse images, including, without limitation, the use of meta-tags for that purpose. Registry Operator/Registrar will refer any sites that are reported to the Registry Operator/Registrar to be in violation of this policy to child safety hotlines like the National Center for Missing and Exploited Children (NCMEC), the Internet Watch Foundation (IWF), or the International Association of Internet Hotlines (INHOPE).

- ***Recommendation 2:*** Each Registry Operator / Registrar include contact information for an "Abuse Contact" so that users can report suspected illegal websites.
- ***Recommendation 3:*** Each Registry Operator / Registrar establish an internal policy/protocol advising staff to forward internal and external reports of child abuse images to the organization's Legal or Compliance Department.
  - It is strongly suggested that members of the organization **DO NOT** access the URL/domain name/website in question.
  - It is strongly suggested that members of the organization **DO NOT FORWARD ANY IMAGES/VIDEOS OR SCREENSHOTS CONTAINING IMAGES OR VIDEOS – BUT SIMPLY PROVIDE THE URL/DOMAIN NAME/WEBSITE.**
- ***Recommendation 4:*** When Registry Operators / Registrars become aware of suspected child abuse images, they expeditiously report the URL/domain name/website directly to a child reporting hotline and provide sufficient contact information to the child reporting hotline to facilitate law enforcement follow up regarding the report submitted.
  - If the reporting organization (or the website) is based in the United States, file a CyberTip report with The National Center for Missing and Exploited Children (NCMEC) at https://report.cybertip.org/index.htm
  - If the reporting organization (or the website) is based in the United Kingdom, file a report with the Internet Watch Foundation (IWF) at: https://www.iwf.org.uk/report
  - If the reporting organization (or the website) is based in a country that is not the United States or the United Kingdom, check the International Association of Internet

Hotlines (INHOPE) reporting page to see if they work with the respective country and report it accordingly, see http://inhope.org/gns/report-here.aspx
    - If the reporting organization (or the website) is not listed in any of the links identified above, submit the report to any of the hotlines you prefer because the various hotlines often work collaboratively so there is generally no need to report to multiple hotlines; a report to one hotline suffices.

- ***Recommendation 4:*** When Registry Operators / Registrars become aware of suspected child abuse images, the organization may document the URLs reported and retain a copy of those URLs for their internal files, in the event the reporting hotline and/or law enforcement follows up with the reporting organization directly and/or for enforcement of any "repeat offender" policies the organization may have. **(It is strongly recommended that Registry Operator/ Registrar does not retain or share any screenshots, images or videos.)**
- ***Recommendation 5:*** Upon contact from a reporting hotline and/or law enforcement, the Registry Operator / Registrar may wish to suspend the domain name, delete the domain name, etc. – pursuant to the organization's policies and protocols.

Aspirational Practices for Organizations that provide Upload, Storage, Search, Hosting, Filtering, or Social Media Services:

If a Registry Operator / Registrar also provides upload, storage, search, hosting, filtering or social media services, and/or an Electronic Service,[4] the organization may wish to consider adopting some or all of the following additional services offered by US and UK child reporting hotlines:

- *NCMEC:* http://www.missingkids.org/Exploitation/
    - *URL Initiative:* NCMEC maintains a list of URLs for active Web pages containing apparent child pornography. By joining the URL Initiative, Electronic Service Providers are provided access to NCMEC's URL list which is updated daily.
    - *PhotoDNA:* This is an image matching technology creates a unique signature for a digital image called a PhotoDNA signature. This signature can be compared with the signatures of other images to find copies of that image. NCMEC and online service providers use PhotoDNA to help find, report and curtail the online circulation of some of the worst known images of child pornography.
    - *NCMEC Hash Value Sharing*: Through the Hash Value Sharing Initiative, U.S. based Electronic Service Providers can partner with NCMEC to receive a list of MD5 hash values which represent the "worst of the worst" images of apparent child pornography.
- *IWF:* Best Practice Guide*: https://www.iwf.org.uk/resources/best-practice-guide*

Image Hash Tag List: The Image Hash Tag List lets parties match known images in order to remove them or prevent them appearing on services. The Image Hashes are categorized to suit international use. Contact HashList@iwf.org.uk for information.

[4] For the United States legal definition of Electronic Service Provider, see: https://www.law.cornell.edu/uscode/text/18/2510

Appendix C: Rogue Pharmacy Abuse Report Proposal

Registry/Registrar Practices for Combating Illegal Internet Pharmacies[5]

Registries and registrars are involved in the provisioning and sale of domain names. From time to time, illegal online pharmacies register domain names and then develop websites on these domain names to try and create a distribution channel for pharmaceuticals in violation of federal and state laws. If given the proper notice information regarding these illegal activities, registrars and registries can take effective action to take down these websites and suspend the domain names from use.

Recommended practices for Registries and Registrars:

- ***Recommendation 1***
  Registrars and registries may acknowledge the ongoing problem of illegal online pharmacies and publicly support the work of organizations such as CSIP and the Alliance for Safe Online Pharmacies (ASOP) and companies involved in combatting the use of domain names for the illegal distribution of drugs and medicines by illegal online pharmacies.
- ***Recommendation 2***
  When registries and registrars become aware of a suspected illegal pharmacy they may refer the domain to a third party provider that verifies the legitimacy of these websites.
- ***Recommendation 3***
  After receiving adequate legal confirmation (pursuant to each organization's own assessment of adequate legal confirmation) that a domain name hosts a website that is used to market and distribute drugs and medicines in violation of applicable laws, registrars and registries may take prompt action. Registries and registrars may take action on confirmed, illegal pharmacies up to and including suspension or deletion of the affected domain(s) in accordance with their internal procedures.
- ***Recommendation 4***
  Registrars and registries also include on their website, contact information for an "Abuse Contact" so that users can report suspected illegal websites for further investigation by a online pharmacy verification provider.

[5] Reprinted with permission from the Center for Safe Internet Pharmacies' "Principles of Participation." Copyright 2016. All Rights Reserved.