Discussion Paper on the Creation of non-binding Best Practices to help Registrars and Registries address the Abusive Registrations of Domain Names

STATUS OF THIS DOCUMENT

This is the Discussion Paper requested by the GNSO Council on 3 February 2011, prepared by ICANN Staff.

SUMMARY

This Discussion Paper is submitted to the GNSO Council on 28 September 2011 pursuant to a Council resolution of 3 February 2011 in response to the Registration Abuse Policies Working Group (RAP WG) final report (20110203).

TABLE OF CONTENTS

1. EXECUTIVE SUMMARY 3

2. INTRODUCTION AND BACKGROUND 5

3. SCOPE CONSIDERATIONS 7

4. THE RAPWG BEST PRACTICES RECOMMENDATION AND ISSUES IDENTIFIED 8

5. PRELIMINARY INVENTORY OF CURRENT OR PROPOSED PRACTICES 19

6. CONCLUSION & PROPOSED NEXT STEPS 20

APPENDIX A 22

1. Executive Summary

1.1. Background

The GNSO Council resolved at its meeting on 3 February 2011 to request a 'discussion paper on the creation of non-binding best practices to help registrars and registries address the abusive registrations of domain names'. The objective of this discussion paper is to analyze the feasibility of engaging in an effort at ICANN to establish best practices with regard to the illicit use of domain names. In addition, it provides a number of recommended next steps for the GNSO Council to consider with regard to taking this effort further.

1.2. Scope considerations

Developing best practices to address abusive domain name registrations falls within the scope of ICANN's mission and core values. The purpose of this paper is to analyze the feasibility of producing non-binding best practices rather than recommendations for binding consensus policies.

1.3. Issues Identified

Section 4 provides an overview of the issues identified in relation to the development and application of best practices, which include:

- What makes a practice a best practice
- Identification and/or creation of best practices
- Defining the non-binding nature of best practices
- ICANN's Role with regards to 'non-binding best practices'
- Resources and process
- Scope of best practices considered
- Maintenance and review of best practices
- Sensitivity of best practices
- Promotion and dissemination of best practices
- Cost, benefit and funding
- Incentives

1.4. Preliminary Inventory of Current or Proposed Practices

Appendix A provides an overview of common or proposed practices identified by Staff that may be candidates for evaluation as “best practices” to address the illicit use of domain names. Registrars, registries and the Internet community at large should identify, based upon experience with their use, which practices are appropriate for consideration as non-binding “best practices” for registries and registrars, or whether, as an alternative, these should instead be considered for future policy work as a binding consensus policy or as amendments to registrar or registry contracts.

1.5. Conclusion and Proposed Next Steps

ICANN Staff supports the recommendation to produce best practices for addressing abusive domain name registrations and believes that such work should be a priority for the ICANN community. If the effort to develop such best practices is appropriately scoped, resourced and implemented, the result may be a more effective response and cooperation among the contracted parties, law enforcement agencies, ICANN and security professionals than exists today. ICANN Staff proposes that the GNSO Council approve the following additional work:

- Creation of a GNSO Working Group to establish the framework for best practices
- Creation of a Cross-Community Technical Group to propose candidate best practices to address the abusive registration of domain names

2. Introduction and Background

2.1 Background

The GNSO Council chartered a Registration Abuse Policies (RAP) Working Group (WG) in February 2009 to identify, amongst others, 'which aspects of the subject of registration abuse are within ICANN's mission to address'. In addition, the GNSO tasked the RAP WG to 'identify and recommend specific policy issues and processes for further consideration'. The RAP Working Group published its Final Report on 29 May 2010. This Final Report included 14 recommendations addressing issues such as cybersquatting, WHOIS access, fake renewal notices as well as a recommendation to create non-binding best practices to help registrars and registries address the illicit use of domain names.

The GNSO Council resolved at its meeting on 3 February 2011 to request 'a discussion paper on the creation of non-binding best practices to help registrars and registries address the abusive registrations of domain names in accordance with the Registration Abuse Policies Working Group Final Report'. This recommendation, adopted unanimously by the RAP WG, reads as follows:

"The RAPWG recommends the creation of non-binding best practices to help registrars and registries address the illicit use of domain names. This effort should be supported by ICANN resources, and should be created via a community process such as a working or advisory group while also taking the need for security and trust into consideration."

2.2 Objective of the Discussion Paper

The objective of this discussion paper is to analyze the feasibility of engaging in an effort at ICANN to establish best practices with regard to the illicit use of domain names as recommended by the RAP-WT. In addition, it provides a number of recommended next steps for the GNSO Council to consider with regard to taking this effort further.

2.3 Community Input

In order to obtain Community input on this topic for inclusion in this discussion paper, a workshop was organized at the ICANN Meeting in Singapore (see http://singapore41.icann.org/node/24623 for further details). An initial outline of the discussion paper was presented (see http://singapore41.icann.org/meetings/singapore2011/presentation-address-abusive-registration-23jun11-en.pdf), followed by different perspectives on the topic. Where appropriate and relevant, these comments have been included in this discussion paper or are referenced. The GNSO Council may want to consider putting this discussion paper out for public comment to obtain further input on the recommendations and the next steps proposed.

3. Scope Considerations

3.1 ICANN's Scope

Developing best practices to address abusive domain name registrations falls within the scope of ICANN's mission and core values. One of ICANN's core values is to preserve and enhance the operational stability, reliability, security, and global interoperability of the Internet. Non-binding best practices that mitigate abusive domain name registrations and DNS misuse (a common derivative effect of abusive registration), if universally adopted by registrars and registries, would serve the interests of the entire Internet community and fall squarely within ICANN's remit, as outlined in the Bylaws and Affirmation of Commitments.

3.2 Registration Abuse vs. Use Abuse

The distinction between "registration abuse" versus "use abuse" has been debated in the context of the deliberations of the Registration Abuse Policies Working Group (see section 4 of the RAP Final Report). However, the purpose of this Discussion Paper is to analyze the feasibility of producing ***non-binding best practices*** rather than recommendations for ***binding consensus policies*** and thus potential best practices to mitigate either form of abuse are considered here. These scope-related issues could be further explored if the GNSO Council desires to initiate policy development activities for binding "consensus policies" applicable to the contracted parties to address the illicit use of domain names in addition to or instead of non-binding best practices.

4. The RAPWG Best Practices Recommendation and Issues Identified

This section of the paper discusses broad, overarching issues related to the development and application best practices, some of which were also identified by the RAP WG, as well as others that have been identified by ICANN Staff and as a result of the workshop that was held at the ICANN meeting in Singapore.

4.1 What makes a practice a best practice?

The Cambridge Dictionaries Online defines a best practice as 'a working method, or set of working methods, which is officially accepted as being the best to use in a particular business or industry, usually described formally and in detail'. Within ICANN or the domain name industry in general, opinions differ as to what constitutes a 'best practice'. For example, who would need to 'officially accept' a practice for it to become a 'best practice'? As outlined in Section 6, Staff encourages the GNSO Council to task a Working Group to clarify the objectives and expected results prior to initiating further activities to produce best practices.

The RAPWG recommended that 'the GNSO, and the larger ICANN community in general, create and support structured, funded mechanisms for the collection and maintenance of best practices'. The RAPWG identified the following goals in its report:

- Develop mechanisms to support the creation and maintenance of best practices efforts in a structured way*;*
- Explore channels that can be used for the dissemination and promotion of best practices to the relevant stakeholders, which might include private and secure channels;
- Develop a mechanism that would allow for working groups and other ICANN bodies to have easy access to existing best practices but also allow for the addition of newly created and adopted best practices as well as the 'retirement' of practices which might become obsolete or are no longer considered effective;
- Develop practices to measure and incentivize the adoption of best practices across the domain industry;

- Develop a process for measuring the adoption and effectiveness of best practices, and for incorporating universal best practices into more formal policies, when deemed appropriate.

Any follow-up activity should take into account the goals identified above and consider that the outcome might serve as the basis for creating and supporting the collection and maintenance of best practices in general.

Other industries and governments globally have developed and maintained best practices as a means of pursuing industry-self regulation rather than a mandatory government regulation scheme. If the Council were to decide to pursue this effort, Staff recommends that a more in-depth survey and analysis of these other approaches be conducted to identify the model that may be best suited for the domain name industry, and would emphasize that this survey and analysis may require a significant investment in staff and community resources and expertise. For example, in 2000, the Australian Government convened a Task Force on Industry Self-Regulation and surveyed the practices internationally.[1] In its Report, it described how OECD has conducted extensive research in this regard. For example, the OECD examined the use of a "Corporate Code of Conduct" as one method of accomplishing self-regulation. The OECD found a variety of codes in operation and drew the following observations[2]:

- For some codes adherence can be a prerequisite for membership in a business association, partnership of stakeholders or for access to recognition marks, such as logos or labels.
- The effectiveness of codes depends on a strong enforcement mechanism.
- Internal monitoring is often needed. A wide range of possible actions, including correction of the conduct in question and termination of existing business relations, can apply to situations of non-compliance.
- Third parties (such as governments) generally do not play a prominent role in code administration.

[1] The Australian Government TaskForce Draft Report on Industry Self -Regulation is posted at http://www.treasury.gov.au/contentitem.asp?ContentID=1131&NavID. Appendix C to this Report includes a description of various International policies of self-regulation at http://www.treasury.gov.au/documents/1123/HTML/docshell.asp?URL=appd.asp

[2] These observations are listed in Appendix C to the Australian Government TaskForce Draft Report.

Some of these observations may be relevant to the development of best practices for registries and registrars for dealing with abusive registrations of domain names. The Australian Government Task Force Draft Report also highlighted the experience with regards to the role of the Council of Better Business Bureaus (CBBB) as a U.S. scheme that supports and administrates self-regulation across numerous industries. Once a business joins the CBBB and commits to the 'Uniform Standards of Membership,' the CBBB plays the following roles:

- Provides an optional dispute resolution scheme to resolve consumer complaints;
- Generates reports about companies for consumers to make an informed choices; and
- Investigates complaints about misleading advertising claims.

The example of the CBBB illustrates some of the options available to the ICANN community in designing a "best practice framework" for dealing with abusive domain name registrations. Staff notes that it would be important for staff or the community to conduct a broader survey of best practices internationally to inform the GNSO Council of the options available to determine which one(s) may be appropriate for the domain name industry.

4.2 Identification and/or creation of Best Practices

Although the RAPWG recommended the 'creation' of non-binding best practices, section 5 of this discussion paper demonstrates that there are (best) practices that have been developed by other ICANN structures and by external parties that address a number of the subjects identified by the RAPWG. For example, over the years, ICANN's Security and Stability Advisory Committee (SSAC) has developed recommendations and suggested techniques to address these subjects, but certain of these recommendations may require field experience before they might emerge as "best practices". Some of the SSAC recommendations were developed having in mind enhancements to the Registrar Accreditation Agreement (RAA), while other SSAC recommendations may be appropriate for adoption as "best practices", Additional work may be involved to make this assessment[3]. Therefore, it might be more appropriate as a first step to categorize and research existing practices that have been considered to be optimal in the past, and existing ICANN recommendations on this topic that might be suitable to

[3] Staff recommends that SSAC should be consulted to understand whether the committee's recommendations were specifically offered as matters for policy consideration or whether certain of these recommendations could be (initially) adopted as part of a best practices initiative and later, following experimentation or adoption as a non-binding practice, become matters for policy consideration.

become “best practices.” Following that, gaps or areas for which no best practices exist can be identified and further work conducted. As part of this step a clear definition of what is meant with ‘abuse’ will be required. This was pointed out by Rod Rasmussen in the ICANN Singapore workshop, who emphasized the importance of specificity when he noted, ‘you have to know what you’re talking about, you have to be very precise in what you’re doing to not cause collateral damage’[4]. General issues that might need further consideration include, amongst others: means to identify trusted abuse reporters; potential liability concerns by registrars / registries in the case of false-positives; how to minimize (and provide remedies for) false-positives; due process; predictability for registrants; definition of what actions comprise a domain name suspension and enumeration of the documentation required when requesting a suspension action.

In addition to the practices identified in section 5, James Bladel[5] from GoDaddy.com, Inc. in his contribution to the workshop suggested that as a starting point, one might evaluate a few basic principles. For example, a registrar or registry should:

- Designate an abuse point of contact (see also SAC 038)
- Consistently apply standard operating procedures
- Assign abuse issues a high priority
- Ensure that registration agreements have the necessary tools to address abuse
- Share information and experiences

In the context of best practices, it might be appropriate to distinguish between high-level principles, such as those outlined above, which are general in nature and less likely to require regular updating or verification, and more detailed practices which can be very granular and may be more likely to require regular updates or periodic reassessment as the threat landscape or mechanisms to address certain threats can change over time. For example, several contributors during the workshop emphasized the importance of flexibility and adaptability when developing best practices to address abuse, especially those that are very specific or technology-specific. These characteristics are necessary to provide

[4] See transcript: http://singapore41.icann.org/meetings/singapore2011/transcript-address-abusive-registration-23jun11-en.pdf

[5] See transcript: http://singapore41.icann.org/meetings/singapore2011/transcript-address-abusive-registration-23jun11-en.pdf

registrars and registries with sufficient agility to respond to changes by miscreants or criminals in tactics or methods the employ to abuse or misuse domain names.

Efforts to create or categorize best practices should identify affected contracted parties, as not all best practices may apply to all parties, as the activities and business models of companies may vary. For example, a practice relevant to providing services to individual registrants may vary from one primarily focused on large business customers.

4.3 Defining the "Non-Binding" Nature of Best Practices

Once developed, "non-binding" best practices could be implemented in a variety of ways, as illustrated below:

- **Not a Mandatory "Consensus Policy."** Non-binding" best practices can mean that if adopted, they are not to be considered mandatory "consensus policies", and ICANN would not be responsible for enforcing them under the applicable contracts with the affected contracted parties.
- **Inclusion of a Registry/Registrar "Code of Conduct" in the RAA or in a registry agreement**. Both the RAA (Section 3.7.1) and the new Registry Agreement for the new gTLD Program reference Codes of Conduct. For example, under the RAA, Registrars agree that: "In the event ICANN adopts a specification or policy, supported by a consensus of ICANN-Accredited registrars, establishing or approving a Code of Conduct for ICANN-Accredited registrars, Registrar shall abide by that Code. " Under Section 2.14 of the Draft New gTLD Registry Agreement, the Registry agrees that: "In connection with the operation of the registry for the TLD, Registry Operator shall comply with the Registry Code of Conduct as set forth in the specification [Specification 9]." If the best practices were to become part of these Codes of Conduct, they could become part of the obligations that ICANN could monitor, and depending upon the actual language, enforce.
- **Standards for a possible "Seals of Approval"[6] administered by ICANN or a designated third party**. Categorization of registrars/registries based upon adoption of Best Practices can serve as a resource to the ICANN community regarding the level of security that a registry/registrar offers. For example, the ICANN community could agree upon a label, rating system or other method of distinguishing registrars that implement best practices.

[6] Note, the concept of a "Seal of Approval" was also discussed extensively in the context of the HSTLD-WG, but no consensus was reached on how such a program should look or could be implemented.

- **Voluntary Adoption, but Enforceable Once Adopted**. A range of best practices could be "endorsed" by ICANN, with various degrees of requirements, from which registrars/registries would "sign up" or adopt those that are most appropriate for its business model and clientele. Once voluntarily adopted, the registrar would commit to abide by that specific best practice and would be accountable for failures to perform to such levels by ICANN or appropriate governmental agencies with jurisdiction over false advertising claims. Incentives, including financial incentives, could be explored to accompany such a model to encourage adoption.

One approach might be to agree that initially, non-binding best practices be treated as 'not a mandatory consensus policy' (see above). Over time, as best practices are demonstrated to be effective and universally adopted, a body of practices could emerge as best practices. These should then be considered for inclusion in a registry/registrar code of conduct that contracted parties agree to adopt or that is adopted as a consensus policy.

4.4 ICANN's Role with regards to 'Non-Binding Best Practices'

Apart from facilitating the development of this best practices work, ICANN could also be involved in maintaining, endorsing, publishing, training, revising, and/or enforcing them. The GNSO community should consider the role that it thinks ICANN should play. The role the GNSO identifies for ICANN will affect the level of resource ICANN requires to engage in this effort. Several of the participants in the workshop expressed their preference for ICANN to take on the role of 'convener' or 'facilitator' for this effort as ICANN is uniquely positioned to bring different parts of the Internet ecosystem together to discuss and work on these issues. Others also pointed to ICANN's role as 'developer' through its community processes or 'repository administrator' and publisher of best practices.

4.5 Resources and Process

The RAP WG recommended that the creation (or categorization, see above) should be done via a community process such as a working or advisory group. Staff believes that this effort may be more effectively accomplished through a group of subject matter experts comprised of representatives from the registrars, registries, the Security and Stability Advisory Committee (SSAC), and invited experts in the field. Once developed, the candidate best practices could then be shared with the broader GNSO community for review, comment and modification as appropriate. In addition, a starting point for further work should be to survey registries and registrars concerning their experience in addressing the abusive registration of domain names and to ask for suggestions they might have to promote and encourage the adoption of best practices amongst registries and registrars in this area. Such a survey should consider input from country code (cc) TLD registries and registrars as some of their procedures on dealing with malicious conduct, either in explicit policies, or through internal procedures might serve as an interesting reference point.

As noted in the GNSO Working Group Guidelines 'all Working Groups are normally expected to operate under the principles of transparency and openness, which means, inter alia, that mailing lists are publicly archived, meetings are normally recorded and/or transcribed'. In this case, exceptions to these Guidelines may be appropriate due to concerns of participants to keep certain information confidential and/or private. Procedures used by the SSAC (see http://www.icann.org/en/committees/security/ssac-operational-procedures-15nov10-en.pdf) or the recently created Joint Security and Stability Analysis Working Group (DSSA-WG) can serve as a model to address such concerns.

4.6 Scope of Best Practices considered

The RAP WG recommended that this effort consider (but not be limited to) these subjects:

- Practices for identifying stolen credentials
- Practices for identifying and investigating common forms of malicious use (such as malware and phishing)
- Creating anti-abuse terms of service for inclusion in Registrar-Registrant agreements, and for use by TLD operators.
- Identifying compromised/hacked domains versus domain registered by abusers
- Practices for suspending domain names
- Account access security management
- Security resources of use or interest to registrars and registries
- Survey registrars and registries to determine practices being used, and their adoption rates.

Section 5 outlines candidate practices that registrars and registries could implement to address certain illicit uses of domain names. These could be tried in the field and, if proven effective, classified as "best practices". It may also be useful to solicit information from registrars, registries, law enforcement, and members of the security community regarding the types of abuse they regularly encounter. Such information could identify additional areas where best practices might be developed and lead to prioritization based upon the types of abuse that are most prevalent.

The importance of registrant education concerning appropriate use of a domain name, appropriate maintenance of registration information, and a clear and complete explanation of actions a registrar will take in case of abusive behavior was highlighted in the workshop. Efforts in this regard should be undertaken in conjunction with any best practice initiative. This could, for example, include recommendations for the inclusion of clear and conspicuous language in terms of service agreements on what a suspension action entails and rights / obligations of a registrant. In this context, it might also be worth noting the recent direction the ICANN Board provided to the 'GNSO, the ALAC and all other parts of the ICANN community to work together to promote the measures outlined in the SSAC's report A Registrant's Guide to Protecting Domain Name Registration Accounts (SAC 044)'[7].

4.7 Other Issues for Consideration

4.7.1 Maintenance and Review of Best Practices

Best practices or effective techniques for detecting and responding to malicious use with peers in the field can be very beneficial. Some best practices are by nature, general commitments of registrars; for example, registrars could agree to provide an abuse point of contact, or they could agree upon criteria for trusting an abuse responder. Other best practices are operational and may involve specific processes; for example, registrars could agree to monitor name server or other domain registration data changes according to a particular method to detect suspicious behavior. Of these, operational best practices may change over time, e.g., in circumstances where criminal or malicious actors attempt to undermine or evade monitoring. The RAP WG noted that, "*no formal mechanisms for collecting such practices, keeping them updated, or disseminating them to all relevant industry participants exists today within the ICANN community. Thus, much of the good work done in these groups is not captured effectively if it is not included in their policy-making outcomes.* This issue was also raised in the Singapore workshop. It will be important for best practice to be maintained under a program that allows for a

[7] See http://www.icann.org/en/minutes/resolutions-25aug11-en.htm#1.2 and ww.icann.org/en/committees/security/sac044.pdf

regular review and revision (where necessary) of best practices to ensure that these remain relevant and effective.

4.7.2 Sensitivity of Best Practices

As also noted by the RAPWG, certain organizations may consider certain of their operation practices in the field of anti-abuse or security to be innovative, sensitive, or proprietary. Such organizations may view these practices as providing a competitive edge against other interveners. Other organizations may not wish to reveal the exact nature of an operational practice because they wish to prevent criminals or malicious actors from adopting new tactics to circumvent them. Some methods to detect or mitigate malicious use are also the subject of academic research or are publicly available. Researchers, interveners and law enforcement collaborate and share techniques and information generously; more importantly, they do not assume that the adversary is incapable of determining the nature of a countermeasure but assume that the countermeasure will be countered by a different attack tactic. As pointed out in the workshop, in certain sectors data and information is shared between organizations via a different setting such as an association, which facilitates data gathering and prioritizing those issues that are most pertinent.

One way to address these concerns is to specify certain practices in “meta terms”, broadly outlining each practice but leaving the details of implementation to be determined by registries and/or registrars. For example, a best practice recommendation could be that bulk registration activity should undergo more scrutiny than individual registrations, as this is a common technique for spammers, but leave the details of implementing this recommendation as well as the threshold for triggering such additional scrutiny for the registrar to determine.

4.7.3 Promotion and Dissemination of Best Practices

Once compiled, it is of utmost importance to promote and widely disseminate these best practices to encourage their adoption. In addition to community or third party initiatives, the role that ICANN can play in this promotion and dissemination (for example, as part of its training programs for registrars and registries or outreach efforts in the different regions), should be considered. As was highlighted during the workshop, time is of the essence, as the domain name industry will likely see many new registries and registrars emerging over the next couple of years. Assisting these new players address abuse through the availability of best practices, sharing of experiences and information should be a key objective of this best practice effort.

4.7.4 Cost, Benefit and Funding

In some cases, adoption of non-binding best practices by registries and registrars will come at some cost. Ultimately, registries and registrars must determine whether and how non-binding best practices may enhance or constrain their respective business models. Those affected are expected to assess the cost versus benefit of the different best practices, and consider trade-offs that might encourage the adoption of the best practices. Input from registries and registrars should be sought in order to identify best practices that are cost effective. In conducting such an assessment, evaluation of the feasibility of the best practice for large vs. small registries and registrars, as well as those for whom English is not the primary language is also encouraged. Some practices, even potentially costly ones, could be collectively viewed as sufficiently important that adoption is recommended despite potential cost increases for all registrants. In such cases, other funding models or incentives (see also next section) could be explored.

4.7.5 Incentives

Additional consideration should be given to incentives and/or subsidies that might facilitate adoption of best practices once developed. In the view of James Bladel[8], the economic model appears upside down for registrars, since being a good actor is considered costly and risky, while doing nothing is just easier. Incentives such as, for example, per domain fee reductions to reward registrars who adopt the best practices and could eliminate the economic disincentive[9]. There might be more of an incentive for registries to address abuse as it directly affects the reputation and brand of a certain gTLD. Pointing to the practices of the financial industry, Martin Sutton[10] observed that working on best practices to address abuse allows the financial industry to protect the industry reputation as a whole as well as the industry itself (from real as well as reputational harm). One of the GNSO community's goals in undertaking this effort could be to affect a change in the culture within the domain name industry

[8] See transcript: http://singapore41.icann.org/meetings/singapore2011/transcript-address-abusive-registration-23jun11-en.pdf

[9] This would require a clear process of how one would qualify for such a reduction, but also what penalties may apply should a registrar no longer follow the best practices after having been rewarded a fee reduction.

[10] See transcript: http://singapore41.icann.org/meetings/singapore2011/transcript-address-abusive-registration-23jun11-en.pdf

where it becomes no longer acceptable to do nothing in response to a credible complaint of domain name misuse.

5. Preliminary Inventory of Current or Proposed Practices

In its research for this paper, Staff conducted an initial survey of current or proposed practices that may be candidates for evaluation as “best practices” to address the misuse or use abuse of domain names. This inventory is attached as Appendix A. Appendix A provides an overview of practices recommended by ICANN’s Security and Stability Advisory Committee (SSAC), as well as practices implemented or recommended by other organizations. Staff believes that these can serve as a starting point for this effort, should the GNSO Council approve next steps as described in Section 6. In Staff’s view, registrars, registries and the Internet community at large should identify, based upon experience with their use, which practices are appropriate for consideration as non-binding “best practices” for registries and registrars, or whether, as an alternative, these should instead be considered for future policy work as a binding consensus policy or an RAA amendment.

6. Conclusion & Proposed Next Steps

As outlined in this discussion paper, there are a number of issues that need further consideration and input. At the same time, substantial efforts have been made by other ICANN entities as well as third parties to develop practices that can serve as a starting point for further work in this area. Ultimately, the real value of any effort related to the creation of non-binding best practices to help registrars and registries address the abusive registration of domain names will lie in the promotion, adoption and assessment of effectiveness of such best practices in addressing abuse.

ICANN Staff supports the recommendation to produce best practices for addressing abusive domain name registrations and believes that such work should be a priority for the ICANN community. If the effort to develop such best practices is appropriately scoped, resourced and implemented, the result may be a more effective response and cooperation among the contracted parties, law enforcement agencies, ICANN and Internet security and operations communities than exists today. Because such activities fall within ICANN's scope and mandate, and could potentially enhance and improve the security and stability of the Internet, ICANN Staff encourages the GNSO Council to approve additional work. Though current staff resources are stretched thin, based on the issues outlined in this discussion paper, we would propose the following next steps for the Council's consideration, subject to scheduling and staff resource constraints:

Creation of a GNSO Working Group to Establish the Framework for Best Practices

- The GNSO Council should convene a GNSO Working Group to develop a framework for the development of Best Practices to address the illicit abuse of domain names by gTLD registries and ICANN-accredited registrars, which addresses the issues identified in this Discussion Paper, including:
    - What makes a practice a 'best practice'
    - Clarify the intended scope of ICANN's Role
    - Defining "Non-Binding"
    - Scope of practices to be considered
    - How to ensure ongoing improvements and updates to agreed best practices

- Promotion and dissemination of best practices

The participation of experts in this area from other organizations such as SSAC and APWG should be strongly encouraged. As a starting point for the efforts of this Working Group, a survey could be conducted of best practices developed internationally in other industries to inform the Working Group of the options available to determine which model(s) may be appropriate for the domain name industry.

Creation of a Cross-Community Technical Group to propose best practices to address the abusive registration of domain names

- In parallel[11] to the GNSO Working Group to establish the framework for best practices, the GNSO Council should convene a cross-community technical group with representatives of the SSAC and GNSO. The objective of this Technical Group would be to review the preliminary inventory of practices in Appendix A, identify additional practices that might qualify to become 'best practices', conduct a survey amongst gTLD registries and ICANN-accredited registrars to gather data on their experience with practices to address the abusive registration of domain names and suggestions they might have to promote and encourage the adoption of best practices amongst registries and registrars in this area. Such a survey should also consider input from country code (cc) TLD registries and registrars as some of their procedures on dealing with malicious conduct, either in explicit policies, or through internal procedures might serve as an interesting reference point. Following completion of these tasks, next steps may include experimenting to see which of the identified practices fit the framework and emerge as "best" practices followed by the sharing of the collection of identified and tested best practices.

[11] Certain activities may be conducted in parallel, although the appointment of liaisons between the two groups may be desirable to ensure communication and co-operation between the two groups. For example, it is to be expected that a framework for the Development of Best Practices needs to be in place before the Cross-Community Technical Group can finalize its recommendations.

Appendix A

The Appendix is organized into the topic areas suggested in the RAPWG Final Report. This initial list has been derived from the following advisories, reports, existing abuse policies and publications:

- Anti-Phishing Working Group: Anti-Phishing Best Practices Recommendations for Registrars (http://www.antiphishing.org/reports/APWG_RegistrarBestPractices.pdf)
- ICANN Security and Stability Advisory Committee: SAC 007, SAC 028, SAC 038, SAC040, SAC044 and SAC 049. (http://www.icann.org/en/committees/security/ssac-documents.htm)
- Anti-Abuse Policies and practices at various registries and registrars.
- Conficker Working Group: Lessons Learned Document. http://www.confickerworkinggroup.org/wiki/uploads/Conficker_Working_Group_Lessons_Learned_17_June_2010_final.pdf
- ICANN Conficker After Action Report. Available: http://www.icann.org/en/announcements/announcement-11may10-en.htm
- MAAWG antiphishing best practices for ISPs and mailbox providers. Available: www.antiphishing.org/reports/bestpracticesforisps.pdf
- Best Practice Recommendations for Minimising Harm (and increasing trust) in small ccTLDs. Available: http://www.cocca.cx/index.php/cocca-news/rfc-minimising-harm.html

This appendix lists and discusses common or observed practices identified by Staff that have been implemented across other companies with similar needs to secure online presence without attempting to distinguish any as “best”. Some of these practices have emerged as best in other industries, whereas others illustrate experimentation or early adoption with practices that may emerge as best practices over time. Adoption of a common and similar strategy by registrars may lead to better practices overall. Registrars, registries and the Internet community at large should identify, based upon experience with their use, which practices are appropriate for consideration as non-binding “best practices” for registries and registrars, or whether, as an alternative, these should instead be considered for future policy work as a binding consensus policy or as amendments to the registrar or registry contracts.

The list in this appendix is not exhaustive, but is intended to illustrate that many enumerations of practices exist today that are relevant to this effort. Staff suggests that as part of any next steps, the drafting team could open a public comment forum or conduct a survey to identify other practices that may be suitable for further review and evaluation.

With regard to the SSAC recommendations covered in this Annex, Staff recommends that SSAC should be consulted to understand whether the committee's recommendations were specifically offered as matters for policy consideration or whether certain of these recommendations could be (initially) adopted as part of a best practices initiative and later, following experimentation or adoption as a non-binding practice, become matters for policy consideration.

Table 1: An overview of Initial Set of Practices Identified

Practice	Year	Developed By	Intended For
Investigate domain registrations/name servers related to known criminal activity.	2008	APWG	Registrars
Establish procedures in place with regard to handling phish domain termination to ensure handling an event in a timely and cost-effective manner.	2008	APWG	Registrars
Proactively use available data to identify and shut down malicious domains	2008	APWG	Registrars
Share fraudulent domain registration information with law-enforcement	2008	APWG	Registrars
Prohibit/minimize use of fast-flux domain	2008	APWG	Registrars
Offer stronger levels of protection against domain name registration service exploitation or misuse for customers who want or need them.	2009	SSAC	Registrars
Expand existing FAQs and education programs they offer to registrants to include security awareness.	2009	SSAC	Registrars
Consider the value of voluntarily having an independent security audit performed on their operations as a component of their security due diligence.	2009	SSAC	Registrars
Study whether registration services would generally improve and registrants would benefit from having an approved independent third party that will, at the request of a registrar, perform a security audit based on a prescribed set of security measures.	2009	SSAC	ICANN and Registrars
Establish Abuse Point of Contact	2009	SSAC	Registrars

Various Anti-abuse policies	2009	PIR, .INFO, Neustar, Godaddy	Registries and registrars
Various measures to reduce phishing threats	2008	SSAC	Registrars
Various measures to reduce Domain Name Hijacking	2005	SSAC	Registries and Registrars
Offer measures to monitor Whois changes	2011	SSAC	Registrars and Registrants
Offer measures to monitor DNS changes	2011	SSAC	Registrars and Registrants
Offer ability for registrant to acquire/download/archive complete zone data	2011	SSAC	Registrars and Registrants

a) PRACTICES FOR IDENTIFYING STOLEN CREDENTIALS

Issue as identified by the RAPWG

Section 6.7 of the working group’s report examined three types of stolen credentials:

1. “Identity credentials” – Credentials that establish identity (e.g. personal identification cards, stored personal information). In general, stolen identity credentials allow a miscreant to assume or impinge the identity of another in order to perpetuate one of their own schemes. This can manifest itself in the use of purloined personal information to make a domain registration appear to be legitimate (e.g. false WHOIS) or in allowing a perpetrator to assume control over access or financial credentials.
2. “Access credentials” – Credentials that control access to computer systems (e.g. username and password, digital certificates). A miscreant can do quite a bit of damage with stolen access credentials. Outside of reselling those credentials, the real value of stolen access credentials lies in what is possible to do with the systems to which those credentials provide access. Two possible attacks seem to be meaningful within the confines of “domain registration abuse”. First are direct attacks against registrar/reseller systems using stolen access credentials for that service. Second, a perpetrator could launch an indirect attack via access credentials to other accounts.
3. “Financial credentials” – Credentials that provide access to financial accounts (e.g. credit and debit cards). Abuses perpetrated with stolen financial credentials are fairly straightforward. The criminal can utilize those credentials to fraudulently register domains and other related resources. This is

quite common practice with criminals today, with most of the domains registered in this manner being used to perpetuate other crime, fraud, and abuse. Such credentials include credit cards, debit cards, on-line banking, alternate payment systems (e.g. PayPal), ACH systems, and other various means for affecting payments for domain name transactions. An interesting aspect for domain name registration via stolen financial credentials versus other types of fraud done via stolen financial credentials is the need to establish domain ownership information (Whois and/or account) and domain deployment characteristics (nameservers) at the time of registration. This allows for some unique techniques to expose fraudulent registrations via stolen financial credentials.

Staff Observations

- Identifying the abuse of "Identity credentials" is a common problem for online merchants, especially for credit card issuers. Practices and systems to screen applicants may exist, but further research would need to be undertaken to identify which among these are suitable for registration services, and which have the potential to emerge as a "best practice".
- Financial, commodities, social networks, telephony providers, and fee-based access services typically use email confirmation as a minimum form of verification when accounts are created or customer profile information is changed. This form of verification is not a panacea for eliminating malicious registrations but it does provide one more measure than widely exists today and would make domain hijackings and unauthorized modification of DNS configuration more difficult for attackers. SAC 040 also lists other measures (machine identification, out of band/voice callback, tokens) financial institutions use. Each such measure adds a layer of defense against impersonation.
- "Access credentials" can be obtained through a variety of ways (e.g. key logging, social engineering), some of which registrars or registries have little control of. It is sometimes not even possible to identify how access credentials have been obtained until the fraud has actually been committed. Thus, the basic assumption for registrars and registries should be that some of these credentials can and will be stolen. Following on from that assumption, registries and registrars should consider how to build controls to minimize the risks. Section 4.6 explores some of these controls further. Staff notes that corporate and global email outsourcing providers now offer "second factor" authentication through a second device (token or registered mobile phone) as a countermeasure against key logging.

- Use of stolen “financial credentials” is a common problem that all electronic merchants face. Various practices exist to detect suspicious activity; for example, credit card companies make extensive use of buying behavior or other individually profiled data to detect fraud. Registrars could similarly monitor purchases that deviate from historical use (a registrant with a small number of domains begins to register what appear to be algorithmically generated strings in bulk) or changes in patterns of behavior (a registrant with a history of rarely making name server configuration changes suddenly changes name server addresses and TTL values with marked frequency). While the specific implementations of such measures might be matters that registrars might consider independently, agreeing in principle to early detection of suspicious activity merits consideration among non-binding practices.

Existing Practices Identified

Examples practices utilized for online merchants include:

- Financial Services Roundtable (2010). Fraud Reduction Program online library, http://www.bitsinfo.org/fraudredLib.html.
- VISA International (2009), Global Visa Card-Not-Present Merchant Guide to Greater Fraud Control, Available at: http://usa.visa.com/download/merchants/global-visa-card-not-present-merchant-guide-to-greater-fraud-control.pdf
- Payment Card Industry Data Security Standard (PCI DSS), https://www.pcisecuritystandards.org/security_standards/documents.php?document=pci_dss_v2-0#pci_dss_v2-0

b) PRACTICES FOR IDENTIFYING AND INVESTIGATING COMMON FORMS OF MALICIOUS USE (SUCH AS MALWARE AND PHISHING)

Issue as identified by the RAPWG

Diligent registrars and registries have procedures for investigating abuse claims. These may include follow-up and documenting problems as a way to protect registrants and minimize false-positives, to avoid risk, or to balance risk with the benefits of stopping malicious behavior. Some registrars and registries may avoid risk by declining to suspend domains at all, or only in the most pressing circumstances. Some may see domain name use as an issue they should not make judgments about at all. Registrars or registry operators generally do not automatically suspend an abusive domain name based on heuristics or abuse blacklists alone. Apparently all require the decision to suspend to be made by an authorized person[12]. Often this function resides with an attorney, a compliance officer, or a specially trained analyst.

Staff Observations

- Registries and registrars could agree on sets and sequences of actions that are involved in abuse claim investigations and agree to implement these through proprietary or using common/openly developed practices

Practices Identified

- **APWG:** Investigate domain registrations/name servers related to known criminal activity. Whenever action is taken to shut down a fraudulent domain registration, action should be taken to identify and shut down other fraudulent registrations that had been submitted by the same registrant (same name, IP, email, address, credit card information, etc.). In addition, name servers that are found to be associated only with fraudulent registrations should be added to a local blacklist and any existing or new registration that uses such fraudulent NS record should be terminated[13].

c) CREATING ANTI-ABUSE TERMS OF SERVICE FOR INCLUSION IN REGISTRAR-REGISTRANT AGREEMENTS, AND FOR USE BY TLD OPERATORS

Issue as identified by the RAPWG

It appears that all registrars and most, if not all registries are already empowered to develop anti-abuse policies and mitigate malicious uses if they wish to do so. In addition, registries may use the Expedited Registry Security Request (ERSR, discussed below) to address threats to the DNS or their TLDs.

[12] See page 55 of the RAPWG Final Report (http://gnso.icann.org/issues/rap/rap-wg-final-report-29may10-en.pdf)

[13] www.antiphishing.org/reports/APWG_RegistrarBestPractices.pdf

Staff Observations

- As also noted in the Registration Abuse Policies Issue Report, there appears to be no uniform approach by registries / registrars to address abuse and there appears to be no universally accepted definition of what constitutes abuse.
- Certain registries or registrars do not publicly disclose how they deal with abuse. However, this does not necessarily mean that they do not deal with complaints of domain name abuse when they arise. A common and public commitment from registrars and registries to deal with abuse in a timely fashion merits consideration.
- There may be benefits to establishing a consistent framework or definition of registration abuse that is applicable across ICANN accredited registries and registrars. In addition, certain providers may define acceptable use policies based on unique or relevant aspects of the services they offer. In examining the possibility of establishing a uniform or consistent best practices framework, it would be useful to understand better whether registries have unique requirements that may call for differing approaches and definitions. Any new framework and/or definition of registration abuse should also be flexible enough to deal with the rapidly changing environment in which registration abuse develops and takes place.

Practices Identified[14]

Many gTLD registries and cctLDs have specific anti-abuse policies. For example, PIR adopted the following anti-abuse policy for .org in 2009[15]:

> Abusive use(s) of .ORG domain names should not be tolerated. The nature of such abuses creates security and stability issues for the registry, registrars and registrants, as well as for users of the Internet in general. PIR defines abusive use of a domain as the wrong or excessive use of power, position or ability, and includes, without limitation, the following:
>
> - Illegal or fraudulent actions;
> - Spam: The use of electronic messaging systems to send unsolicited bulk messages. The

[14] Citations included in this section from particular registry and registrar policies should not be considered as endorsement of any single practice.

[15] See PIR (.ORG) anti-abuse policy: http://www.pir.org/why/anti_abuse_policy. This policy is very similar to the .INFO anti-abuse policy: http://www.info.info/information/anti-abuse-policy.

term applies to e-mail spam and similar abuses such as instant messaging spam, mobile messaging spam, and the spamming of Web sites and Internet forums. An example, for purposes of illustration, would be the use of email in denial-of-service attacks;

- Phishing: The use of counterfeit Web pages that are designed to trick recipients into divulging sensitive data such as usernames, passwords, or financial data;
- Pharming: The redirecting of unknowing users to fraudulent sites or services, typically through DNS hijacking or poisoning;
- Willful distribution of malware: The dissemination of software designed to infiltrate or damage a computer system without the owner's informed consent. Examples include, without limitation, computer viruses, worms, keyloggers, and trojan horses.
- Fast flux hosting: Use of fast-flux techniques to disguise the location of Web sites or other Internet services, or to avoid detection and mitigation efforts, or to host illegal activities. Fast-flux techniques use DNS to frequently change the location on the Internet to which the domain name of an Internet host or name server resolves. Fast flux hosting may be used only with prior permission of PIR;
- Botnet command and control: Services run on a domain name that are used to control a collection of compromised computers or "zombies," or to direct denial-of-service attacks (DDoS attacks);
- Distribution of child pornography; and
- Illegal Access to Other Computers or Networks: Illegally accessing computers, accounts, or networks belonging to another party, or attempting to penetrate security measures of another individual's system (often known as "hacking"). Also, any activity that might be used as a precursor to an attempted system penetration (e.g., port scan, stealth scan, or other information gathering activity).

Pursuant to Section 3.6.5 of the RRA, PIR reserves the right to deny, cancel or transfer any registration or transaction, or place any domain name(s) on registry lock, hold or similar status, that it deems necessary, in its discretion; (1) to protect the integrity and stability of the registry; (2) to comply with any applicable laws, government rules or requirements, requests of law enforcement, or any dispute resolution process; (3) to avoid any liability, civil or criminal, on the part of PIR, as well as its affiliates, subsidiaries, officers, directors, and employees; (4) per the

> terms of the registration agreement or (5) to correct mistakes made by PIR or any Registrar in connection with a domain name registration. PIR also reserves the right to place upon registry lock, hold or similar status a domain name during resolution of a dispute.
>
> Abusive uses, as defined above, undertaken with respect to .ORG domain names shall give rise to the right of PIR to take such actions under Section 3.6.5 of the RRA in its sole discretion.

Some registries, for example .biz pose certain registration restrictions[16]:

> 1. **Registrations in the .biz TLD must be used or intended to be used primarily for bona fide business or commercial purposes; and**
> 2. Registrations in the .biz TLD must comply with the Uniform Dispute Resolution Policy ("UDRP"), as adopted and as may be amended by the Internet Corporation of Assigned Names and Numbers.
>
> ….
>
> For illustration purposes, the following *shall not* constitute a "bona fide business or commercial use" of a domain name:
>
> 1. Using or intending to use the domain name exclusively for personal, noncommercial purposes; or
> 2. Using or intending to use the domain name exclusively for the expression of noncommercial ideas (i.e., registering xxxsucks.biz exclusively to criticize or otherwise express an opinion on the products or services of ABC company, with no other intended business or commercial purpose);
> 3. **Using the domain name for the submission of unsolicited bulk e-mail, phishing, pharming or other abusive or fraudulent purposes.**

Finally, many registrars such as GoDaddy.com, Inc. also have provisions in their Terms of Service to address specific types of abuse (e.g. medical spam):

[16] See .BIZ Registry Agreement, Appendix 11. Registration Registrations. Available at: http://www.icann.org/en/tlds/agreements/biz/appendix-11-08dec06.htm

You will not use this Site or the Services found at this Site in a manner (as determined by GoDaddy in its sole and absolute discretion) that:

a. Is illegal, or promotes or encourages illegal activity;
b. Promotes, encourages or engages in defamatory, harassing, abusive or otherwise objectionable behavior;
c. Promotes, encourages or engages in child pornography or the exploitation of children;
d. Promotes, encourages or engages in hate speech, hate crime, terrorism, violence against people, animals, or property, or intolerance of or against any protected class;
e. Promotes, encourages or engages in any spam or other unsolicited bulk email, or computer or network hacking or cracking;
f. Violates the Ryan Haight Online Pharmacy Consumer Protection Act of 2008 or similar legislation, or promotes, encourages or engages in the sale or distribution of prescription medication without a valid prescription;
g. Infringes on the intellectual property rights of another User or any other person or entity;
h. Violates the privacy or publicity rights of another User or any other person or entity, or breaches any duty of confidentiality that you owe to another User or any other person or entity;
i. Interferes with the operation of this Site or the Services found at this Site
j. Contains or installs any viruses, worms, bugs, Trojan horses or other code, files or programs designed to, or capable of, disrupting, damaging or limiting the functionality of any software or hardware; or
k. Contains false or deceptive language, or unsubstantiated or comparative claims, regarding Go Daddy or Go Daddy’s Services.

d) IDENTIFYING COMPROMSED / HACKED DOMAINS VERSUS DOMAINS REGISTERED BY ABUSERS

Issue as identified by the RAPWG

About 81% of domains used for phishing are compromised or hacked by phishers, and the registrants are not responsible for the phishing. These domains should therefore not be suspended, and the hosting provider must usually perform mitigation. "Malicious" domain registrations totaled about 5,591 domain names in all gTLDs and ccTLDs worldwide in the first six months of 2009. This was about 18.5% of the domain names involved in phishing.

Staff Observations

Practices for distinguishing compromised domains vs. maliciously registered domains are not well-documented nor published in condensed forms by organizations that detect and respond to domain abuse and misuse. However we note the following based on our preliminary research that the following organizations track and catalog malicious registrations and compromised domains:

- The Anti-Phishing Working Group (APWG) publishes phishing statistics bi-annually. In this publication, it distinguishes hacked domains vs. maliciously registered domains, so the APWG appears to have a procedure to separate the two.
- Many of the maliciously registered domains are generated algorithmically. Academic researchers Yadav, et al[17] have developed methodologies to detect these algorithmically generated malicious domain names used in various botnets (Conficker, Kraken, and Torpig) with reasonable success.
- The existence of many URL and domain blocklists indicates that interveners regularly distinguish malicious domains from compromised domains.

Staff recommends that the organizations who maintain such lists be contacted and asked to share their methodologies (to the extent willing) so that a set of principles or practices for detecting malicious domains might be documented and considered by registrars for experimentation or adoption.

[17] See "Detecting Algorithmically Generated Malicious Domain Names" by Yadav, Reddy and Ranjan. (2010) www.ece.tamu.edu/~reddy/papers/imc2010-yadav.pdf

e) PRACTICES FOR SUSPENDING DOMAIN NAMES

Issue as identified by the RAPWG

The decision to suspend a domain name is up to the discretion of the registrar or registry operator, as per their terms of service. Suspending domain names can involve risk if done erroneously. Registrars and registry operators especially wish to avoid suspending the domain names of innocent parties (a "false-positive"). A mistake can take an innocent registrant's Web site and e-mail offline and potentially cause significant economic damage and other problems for the registrant. In turn, the registrar or registry operator may risk legal action, and may further face customer service and public relations problems.

Staff Observations

The risks or consequences of unacceptable rates of false positives are an important consideration for registrars. Other industries and professions (e.g., medical, financial, airline) manage this risk in environments where "zero false positive" is understood as unachievable. Development of a risk framework that weights the likelihood of false positive against the consequence or impact beyond the registrant of continued resolution of a domain name and provides acceptable circumstances for temporary suspension of a domain or name resolution merits consideration. Staff also observes that:

- Phishing sites typically do most of their damage in the first few hours of the phishing operation[18]. Thus, it is critical that action be taken to prevent further malicious activity via the domain be as quickly as possible once the registrar/registry is notified and has confirmed the criminal activity associated with that domain.
- In relation to false-positives, staff recommends that data be gathered regarding the frequency of false positive reporting as well as a census of actual cases where a false positive resulted in loss and litigation. These data should be compared against other industries and professions to understand how the actual risk or real losses associated with false positive domain suspensions relates to the common speculation.
- Various organizations/companies specialize in identifying these malicious domains and will contact registrars/registries for shutdown. However, The RAPWG report noted that "there are

[18] See Sheng, S., Wardman, B., Warner, G., Cranor, L., Hong, J ., And Zhang, C. An empirical analysis of phishing blacklists. In Proceedings of the 6th Conference in Email and Anti-Spam (Mountain view, CA, July 16 - 17 2009). CEAS 2009.

no registrars or registry operators that trust heuristics or abuse blacklists in order to automatically suspend abusive domain names. All required the decisions to be made by an authorized person." Further discussion to understand the impact of having authorization performed outside an automated process, the cost of such intervention, and how the impact or cost might be lessened or shared across vested parties.

- There is no common convention across registrars for what "suspending a domain" entails. Staff observes at least these three variations: (1) some registrars put the domain on hold but the hold period varies, (2) some registrars release the domain to the available pool (where the abusing party could possibly register it again), (3) some registrars change the domain registration record (the registrar becomes the contact), and absent a WhoWas service, this may inhibit investigations. Development of a common set of "suspension actions" should be part of the work done to develop "best practices" in this regard.

Practices Identified

[The following sections summarizes Anti-Phishing Working Group's best practice for registrars]

APWG recommended registrars establish procedures in place with regard to handling phish domain termination to ensure handling an event in a timely and cost-effective manner. Some of these procedures include:

1. Identify the company internal team that addresses phishing inquiries and provide them with procedures and guidance policies (if possible, this should be a 24x7 team since phishing inquiries can arrive at any time)
2. Specify the evidence required to verify that a site is being used for phishing. This may include having your team perform an independent verification of the organization reporting the phishing site or investigate whether the site is being used for malicious purposes. (The APWG is working on a process to accredit phishing site takedown providers. Once that process is in place, registrars can use it to confirm an organization has been accredited to identify phishing sites.)
3. Outline the steps to take to shut down the domain
4. Outline the procedure for evidence collection, evidence storage, and contacting law enforcement

APWG: Proactively use available data to identify and shut down malicious domains

There are numerous sources that can provide information to help in identifying malicious activity. The APWG can provide a daily feed to registrars listing all of the phishing URLs identified by the APWG community for cross-reference. Entities such as the Spam and Open Relay Blocking System (SORBS) Dynamic User and Host List can provide networks associated to dial-up, DSL, and cable networks that are more likely to be abused. The Composite Block List (XBL) may indicate fraud. Optimally, a registrar would check against this information at DNS set-up or modification time; however, periodic scanning should return good results.

APWG: Share fraudulent domain registration information with law-enforcement

Whenever action is taken to shut down a fraudulent domain registration, appropriate law enforcement authorities should be notified and all available information about the deceptive registration should be shared with them. Such information includes registrant IP addresses used during registration or modification of the domain record, credit card information, name, address, e-mail, company name, and all other available data.

f) ACCOUNT ACCESS SECURITY MANAGEMENT

Issue as identified by the RAPWG

No further information on this issue as part of the RAPWG Final Report.

Staff Observations

- SAC 040[19] identifies several issues related to registration account attacks, including: 1) All an attacker needs to gain control of an organization's entire domain name portfolio is a user account and password; 2) Attackers need only guess, phish, or apply social engineering techniques on a single point of contact to gain control of a domain registration account; 3) Attackers scan domain account registration and administration portals for web application vulnerabilities (e.g., SQL injection). A successful exploit of vulnerable application code can result

[19] See SAC 040, "Measures to Protect Domain Registration Services Against Exploitation or Misuse", Available at: http://www.icann.org/en/committees/security/sac040.pdf.

in the disclosure of account credentials for many domain accounts; 4) Email is the preferred and often the only method by which some registrars attempt to notify a registrant of account activity; 5) Attackers can block delivery of email notifications to targeted registrants by altering DNS configuration information so that email notifications will not be sent to any recipient in the domains the attacker controls through a compromised account; and 6) Access to and the ability to modify contact and DNS configuration information for all the domains in a registration account is commonly granted through a single user account and password; and 7) Even when unauthorized modification of DNS information is discovered quickly, the process of restoring DNS information to correct for a malicious configuration can be a lengthy one that is inherent in the distributed nature of the DNS and related to time to live (TTL) values.

- Based on case studies of real account compromise incidents, SAC 040 recommended a set of account access and management practices to prevent domain account and DNS hijacking, protect access to domain portfolio, and protect DNS configuration information from abuse.

Practices Identified

Practices for Registrars:

- SAC 040 Recommendation 1: Registrars are encouraged to offer stronger levels of protection against domain name registration service exploitation or misuse for customers who want or need them. Measures includes registration verification, improve password-based authentication system, system registration, multi-factor authentication, challenge systems, per domain access controls, multiple unique points of contact, change notifications or confirmations, multi-recipient notifications, multiple delivery methods for critical correspondence engaging the customer, inform the customer about the kinds of security measures provided by the registrar, individually or bundled. For detailed lists of measures enumerated, see http://www.icann.org/en/committees/security/sac038.pdf.
- SAC 040 Recommendation 2: Registrars should expand existing FAQs and education programs they offer to registrants to include security awareness. Registrars should make information concerning the services they offer to protect domain registration accounts more accessible to customers so that they can make informed decisions regarding protective measures when they choose a registrar.
- SAC 040 Recommendation 3: Registrars should consider the value of voluntarily having an

independent security audit performed on their operations as a component of their security due diligence.

- SAC 040 Recommendation 4: ICANN and registrars should study whether registration services would generally improve and registrants would benefit from having an approved independent third party that will, at the request of a registrar, perform a security audit based on a prescribed set of security measures. ICANN would distinguish registrars that voluntarily satisfy the benchmarks of this security audit through a trusted security mark program that is implemented in a manner similar to the way that SSL certificate issuing authorities provide trust marks or seals for web site operators who satisfy that authority's security criteria.

g) SECURITY RESOURCES OF USE OF INTEREST TO REGISTRARS AND REGISTRIES

Staff has not identified any security resources at this stage and would request input on the scope of these security resources (see conclusion and proposed next steps).

h) SURVEY REGISTRARS AND REGISTRIES TO DETERMINE PRACTICES BEING USED, AND THEIR ADOPTION RATES

As noted in the discussion paper, any follow-up activity should commence with requesting feedback and input from registries and registrars, including best practices being used and adoption rates.

i) OTHER PRACTICES

Issue as identified by the RAPWG

No further information on this issue as part of the RAPWG Final Report.

Staff Observations

- In addition to the subjects identified by the RAPWG, Staff also identified the following that address, amongst others, phishing, abuse point of contact and domain name hijacking.

Recommended Practices Identified

How registrars can reduce phishing threats (SAC 028). SSAC recommends that registrars do the following:

- Only include information necessary to convey the desired message in customer correspondence. Do not include customer account numbers, identities, and (generally) registration information. These create opportunities for phishers to personalize email.
- Avoid using hyperlink references in correspondence with customers. Phishers commonly disguise links to redirect users from a legitimate page to a spoofed one.
- Warn customers against clicking on hyperlinks included in any correspondence, in text or image fashion. Include statements in the message bodies of correspondence you send such as, "To protect against phishing, please type the following web address into the address bar of your web browser" or "Do not trust links in email. Always type a web address into your browser's address bar".
- Raise awareness that registrars are targets for phishing attacks. Provide (or expand existing) FAQ pages to call attention to registrar impersonation phishing, the threats these phishing attacks pose, measures you are taking to deter phishing and measures your customers can take to detect and avoid falling victim to such attacks. Explain the type of information you will include in email correspondence and in particular, identify the types of information that you will never include in correspondence so that customers have a basis for assessing whether correspondence they receive is legitimate or suspicious.
- Provide a means for a customer to report suspected phishing attacks, either directly, or in cooperation with an organization that encourages submission of suspected scam and fraud emails and maintains a repository of phishing emails.
- Consider implementing a form of email non-repudiation of origin for customer correspondence, such as a digital signature.

Abuse Point of Contact (SAC 038)

SSAC recommends that registrars and resellers assist in the investigation and mitigation of abuses and illegal activities in cases where attackers exploit domain name resolution and registration services. We recommend that the GNSO consider the following and act accordingly:

- Each registrar should provide an abuse contact.
- The abuse point of contact should be responsive and effective. The abuse contact must answer the phone and email quickly, people handling abuses must be empowered to take effective action, and they must have well defined criteria for their actions. The GNSO should consider the criteria for availability and access to the abuse contact (e.g., 24x7 or normal business hours), and the mean time to respond to a complaint. ICANN and registrars should consider how compliance would be evaluated for these metrics.
- Registrars should provide complainants with a well-defined, auditable way to track abuse complaints (e.g. a ticketing or similar tracking system).
- Registrars should publish abuse contact information.
- The registrar identified in the sponsoring registrar field of a Whois entry should have an abuse contact listed prominently on its web page. To assist the community in locating this page, SSAC recommends that registrars consider a uniform naming convention to facilitate (automated and rapid) discovery of this page, i.e., http://www.<registar>.<TLD>/abuse.html.
- Registrars should provide ICANN with their abuse contact information and ICANN should publish this information at http://www.internic.net/regist.html.
- The information a registrar publishes for the abuse point of contact should be consistent with contact details currently proposed as an amendment to Section 3.16 of the RAA. Each contact method (telephone, email, postal address) should reach an individual or organization able to attend to an abuse claim; for example, no contact should intentionally reject postal or email submissions.
- The GNSO should identify what constitutes appropriate abuse contact information, how and where the information is published. SSAC calls attention to RFC 2142, Mailbox Names for Common Services, Roles, and Functions and suggests that registrars make use of the naming conventions therein.
- Abuse point of contact information should be made available in a uniform, machine-readable format. The GNSO should decide whether one or all of these publishing options are appropriate.
- ICANN and registrars should work cooperatively with the community to determine appropriate measures to safeguard against false complaints. The details of what constitutes abuse and what protections must be provided against false complaints must be worked out with the registrar

community and the user community. Equally, the criteria for how quickly complaints have to be answered need to be worked out with the registrar and user communities. The GNSO should undertake this activity as part of a comprehensive study of registration abuse.

- ICANN should periodically (no less frequently than annually) verify that these contacts are accurate.

Domain Hijacking

SSAC recommends the following measures for registrars and registries to protect against domain hijacking:

Recommended Practices for Registrars:

- SAC 007 Recommendation 3: Under the current transfer policy, a losing registrar notifies a registrant upon receiving a pending transfer notice from the registry at its option. Registrars should investigate whether making this notice a mandatory action would reduce hijacking incidences.
- SAC 007 Recommendation 4: Registrars should make contact information for emergency support staff available to other registrars, agents of registrars (resellers), and registry operators. Specifically, registrars should provide an emergency action channel. The purpose of this channel is to provide 24 x 7 access to registrar technical support staff that are authorized to assess an emergency situation, establish the magnitude and immediacy of harm, and take measures to restore registration records and DNS configuration in circumstances which merit such intervention.
- SAC 007 Recommendation 5: Registrars should identify evaluation criteria a registrant must provide to obtain immediate intervention and restoration of domain name registration information and DNS configuration. Registrars should define emergency procedures and policy based on these criteria. This policy would complement the Transfer Dispute Resolution Policy (TDRP) and must not undermine or conflict with those policies.
- SAC 007 Recommendation 7: Registrars should investigate additional methods to improve accuracy and integrity of registrant records. More frequent or alternate communications might assist registrants in keeping their information up to date. Registrars should also acquire emergency contact information from registrants for technical staff who are authorized and able

to assist in responding to an urgent restoration of domain name incident.

- SAC 007 Recommendation 8: Registrars should improve registrant awareness of the threats of domain name hijacking and registrant impersonation and fraud, and emphasize the need for registrants to keep registration information accurate. Registrars should also inform registrants of the availability and purpose of the Registrar-Lock, and encourage its use. Registrars should further inform registrants of the purpose of authorization mechanisms (EPP authInfo), and should develop recommended practices for registrants to protect their domains, including routine monitoring of domain name status, and timely and accurate maintenance of contact and authentication information.

Recommended Practices for registries

- SAC 007 Recommendation 1: Registries should ensure that Registrar-Lock and EPP AuthInfo are implemented according to specification. In particular, registries should confirm that registrars comply with the transfer policy and do not use the same EPP AuthInfo code for all domains they register.
- SAC 007 Recommendation 2: Registries and registrars should provide resellers and registrants with Best Common Practices that describe appropriate use and assignment of EPP AuthInfo codes and risks of misuse when the uniqueness property of this domain name password is not preserved.
- SAC 007 Recommendation 6: ICANN, the registries, and the registrars should conduct a public awareness campaign to identify the criteria and the procedures registrants must follow to request intervention and obtain immediate restoration of a domain name and DNS configuration.