

Staff Notes

Registrar Accreditation Agreement

Additional Amendments

14 October 2009

Status of the Document

Notes to the ICANN community prepared by ICANN Staff.

Summary

This document identifies considerations arising from the GNSO Council's Resolution 3 September 2009, resolving that additional work on further amendments to the Registrar Accreditation Agreement (RAA) be conducted, and to identify those on which further action may be desirable. The additional work is intended to build on the 2009 RAA as approved by the ICANN Board at its 21 May 2009 meeting. This document discusses ICANN's compliance activities related to the RAA, and identifies specific subjects to be considered as the ICANN community begins to discuss possible additional amendments to the RAA.

Table of Contents

Introduction	3
Background	3
Category 1: Potential New RAA Obligations to Address Internet Community Concerns about the DNS	5
1.1. Prohibition of Registrar Cybersquatting	5
1.2. Malicious Conduct Involving the DNS	6
1.3. Privacy/Proxy Services and Resellers	8
1.4 Additional Information on Registrars and their Affiliates	10
Category 2: Amendments to RAA to Clarify Agreement and Promote Registrar Compliance with Existing RAA Obligations	12
2.1. WHOIS Inaccuracy Claims	12
2.2. Examination by ICANN of Registered Name Holder Registration Data	14
2.3. Termination of RAA by ICANN	15
2.4. Business Dealings with Registered Name Holders	16
2.5. Manner of Establishment of New and Revised Specifications and Policies	17
2.6. Insurance	18
2.7. Arbitration	19
2.8. Administration of Contracts	21
2.9. Privacy and Security of Registrant Account Records	22

Introduction

The purpose of this document is to provide suggestions to be considered by the Council in its efforts to identify additional changes to the RAA. As a party to the RAA, ICANN is responsible for enforcing its terms. This document is intended as guidance to assist the ICANN community in understanding issues that have been the subject of RAA related complaints to ICANN, and provides suggestions for amendments that could improve agreement clarity and enhance compliance activities.

An ICANN cross-functional team produced the attached list of possible RAA amendment topics for consideration by the GNSO Working Group. The list is divided into two categories. Category One describes recommended RAA amendments to address Internet community DNS concerns that have been forwarded to ICANN. These include: registrar cybersquatting, malicious conduct involving the DNS, privacy/proxy services and resellers, and additional information on registrars and their affiliates.

Category Two describes possible RAA amendments to improve agreement clarity and promote registrar compliance with existing RAA obligations, including the subjects of: handling WHOIS inaccuracy claims, facilitation of examination registrar records by ICANN, conditions for termination of the RAA by ICANN, defining the time in which a registered name holder must disclose the licensee identity to avoid liability, manner of establishment of new and revised specifications and policies in a restructured GNSO, insurance requirements, arbitration details, and streamlining registry accreditation.

Within the categories, each possible RAA Amendment is explored through a three-step process: a description of the issue, a concise proposal or recommendation, and a review of potential options available to the GNSO Working Group.

Background

In March 2009, the GNSO Council approved a set of amendments to the RAA developed by ICANN staff and Registrars, taking into account substantial input from the community. On 21 May 2009, ICANN's Board of Directors approved the RAA amendments and directed staff to implement the amendments.

Since the May 2009 approval by the ICANN Board, ICANN staff has been working to implement the 2009 RAA. As a result of incentives and registrar/ICANN cooperation, registrars representing over 87.3% of all gTLD registrations have signed or requested the 2009 RAA as of

10 October 2009. All ICANN accredited registrars will operate under the 2009 RAA within five years.

Using tools provided in the adopted amendments, ICANN will continue to explore ways to identify registrar noncompliance early, take action swiftly to identify and cure breaches and, if indicated, terminate agreements with those registrars that violate the agreement.

In developing the implementation details for the launch of the New gTLD Program, ICANN has produced a number of suggested revisions to the Base Registry Agreement that are similar in nature to the recent amendments to the RAA. Likewise, this document imports some of the concepts and community discussions that have occurred concerning the new gTLD program and suggests similar possible improvements to the RAA. Many of the principles identified in the new gTLD program, such as those addressing malicious conduct, cybersquatting, and enhanced verification, are equally applicable to the RAA.

The contractual framework that governs ICANN's relationships with its registrars has been improved by the 2009 RAA amendments. The ICANN community has achieved measurable success in registrant protections, and the GNSO has resolved to continue to improve and innovate in the area of registrant protections and the RAA. The potential RAA amendments presented in this document are intended to enhance ICANN's and registrar's ability to attain compliance with the contract.

Category 1: Potential New RAA Obligations to Address Internet Community Concerns about the DNS

1.1. Prohibition of Registrar Cybersquatting

Statement of Problem:

ICANN has received complaints about registrars who are allegedly engaged in cybersquatting either directly or through affiliates. The RAA does not explicitly identify cybersquatting as a basis for terminating the RAA. In many countries, including the United States, laws exist to address cybersquatting, spamming, and other malicious activity that can result in harm to Internet users, trademark holders and others.

Recommendation:

Incorporate terms in the RAA that explicitly prohibit cybersquatting.

Implementation Options:

1. Amend the RAA to specifically prohibit registrars and their affiliates from engaging in cybersquatting, including an evidentiary standard to determine breach of the prohibition against cybersquatting (e.g., evidence of bad faith intent to profit from infringing domains, knowingly take actions inconsistent with the UDRP, or a final court order, preliminary injunction, or arbitration decision based on a specific violation(s) of applicable national law or governmental regulations relating to cybersquatting).
2. Currently, the violation of RAA Section 3.7.2 entitled “applicable laws and government regulations” by registrars is a breach of the RAA. Under section 5.3.4 a registrar has fifteen working days after ICANN gives notice of a breach to cure. A violation of RAA Section 3.7.2 is the type of offense that should result in immediate termination of the RAA. Therefore, insert in RAA Section 5.3.2 the right to immediately terminate the RAA when a registrar violates RAA Section 3.7.2 or the prohibition against cybersquatting.
3. Adopt a Registrar Code of Conduct (RAA, Section 3.7.1) that incorporates provisions to achieve similar results.
4. Amend the RAA to require a registrar to provide to ICANN a list of pending litigation, UDRP proceedings and arbitrations alleging cybersquatting or other domain registration-related complaints in cases where the registrar or its affiliates is the registered name holder) within sixty days after registrar receives notice of the complaint.

1.2. Malicious Conduct Involving the DNS

Statement of Problem:

The Internet community frequently voices concern to ICANN about malicious conduct and, in particular, the extent to which these attacks take advantage of domain registration and name resolution services. Consumers, law enforcement, representatives from government and others are asking ICANN, its registries and registrars to monitor the increasing levels of malicious conduct and, when appropriate, take reasonable steps to detect, block and mitigate such conduct. ICANN and its registrars are often viewed by the public as the key to successfully resolving malicious conduct because of ICANN's contractual relationships with registrars and registrars' direct customer relationships with certain registrants who misuse the DNS. It would be difficult to define precise rules to govern what actions all registrars should have to take in response to every complaint about malicious conduct involving use of a domain name, but as a first step registrars could be required to be responsible for investigating and reporting back on its handling of credible reports about malicious conduct.

Recommendation:

Incorporate a provision in the RAA establishing a duty of registrars to investigate and report back to ICANN on what actions the registrar has taken in response to reports received from a credible third-party demonstrating illegal malicious conduct involving domain names.

Implementation Options:

1. Insert language in the RAA requiring registrars to investigate within a time certain, any report demonstrating harm from illegal malicious use of a domain received by registrar from ICANN or other credible sources such as law enforcement agencies, security professionals, trademark owners, attorneys or consumer protection agencies.
2. An automatic email response by registrars would not be considered sufficient investigation and response. The registrar should state how it has responded or will respond to the inquiry, or in the alternative, why it believes a response is not required.
3. Adopt a Registrar Code of Conduct (RAA, Section 3.7.1) that incorporates provisions to achieve similar results.
4. Registrars to provide and maintain complete and accurate contact information for a point of contact for contractual compliance matters.

5. Registrars to provide and maintain complete and accurate contact information for a point of contact for malicious conduct, including allegations of fraud and domain name abuse (as recommended by SSAC 38 <<http://www.icann.org/committees/security/sac038.pdf>>).

1.3. Privacy/Proxy Services and Resellers

Statement of Problem:

1.3.1. RAA Section 3.4.1 does not require a registrar to escrow privacy or proxy registration data. For example, a registrar can display a conspicuous notice to its customers advising them that in the event the customer/registered name holder chooses to use a privacy or proxy service when registering a domain name, that the registrar will not escrow their data. Likewise, under RAA Section 3.12.4, a reseller can also voluntarily choose not to escrow privacy or proxy registration data by providing a conspicuous notice to its customers at the time the customers elects to utilize a privacy or proxy service. Failure to escrow privacy or proxy registration data can result in harm to the users of privacy and proxy services.

1.3.2. RAA section 3.7.7.3 requires that "Any Registered Name Holder that intends to license use of a domain name to a third party is nonetheless the Registered Name Holder of record and is responsible for providing its own full contact information and for providing and updating accurate technical and administrative contact information adequate to facilitate timely resolution of any problems that arise in connection with the Registered Name. A Registered Name Holder licensing use of a Registered Name according to this provision shall accept liability for harm caused by wrongful use of the Registered Name, unless it promptly discloses the current contact information provided by the licensee and the identity of the licensee to a party providing the Registered Name Holder reasonable evidence of actionable harm." These provisions are intended to ensure that the contact data listed in a Registrar's Whois output is "adequate to facilitate timely resolution of any problems that arise in connection with the Registered Name." ICANN has received numerous complaints regarding difficulties with the "timely resolution of any problems" in cases where the registrant of record has licensed the use of the domain to a third party (i.e., where the registrant is a "proxy" that has licensed the use of the name to the customer of the proxy service). In order to further the goal of facilitating timely resolution of problems that arise in connection with domain registrations, the RAA could be amended to try to avoid cases where a proxy registrant might hinder the resolution of problems by failing to diligently respond to reported problems or forward such reports to the registrant's licensee, or both.

Recommendation:

1.3.1. Insert provisions in the RAA that require a registrar and its resellers to escrow privacy or proxy registration data, and at a minimum, disclose the points of contact for privacy or proxy service providers and a description of the privacy or proxy services offered to their customers.

1.3.2. Insert in RAA Section 3.7.7.3 provisions that require privacy or proxy services to forward allegations of malicious conduct, cybersquatting, and other illegal activities to privacy or proxy service customers.

Implementation Options:

1.3.1.1. Develop and implement the program in RAA Section 3.12.4 of the RAA giving ICANN the ability to establish or “make available a program granting recognition to resellers that escrow privacy or proxy registration data”. Create a similar contractual provision in RAA Section 3.4.1 for registrars.

1.3.1.2. Require registrars on an annual basis to provide a list of privacy or proxy registration services, including points of contact for privacy or proxy service providers and a description of the services provided or made available by a registrar to its customers. This information could be provided either directly to ICANN or published by a registrar on its web site. This requirement would assist ICANN in determining compliance with RAA Section 3.4.1 related to escrow of Whois information.

1.3.2.1. Require privacy/proxy registration services to forward correspondence to its customer related to specific disputes or alleged disputes involving the domain name.

1.3.2.2. Require privacy/proxy registration services to provide to ICANN, upon its request, “point of contact” for any privacy or proxy registration services offered or made available to registrar's customers that are responsible for investigating and responding to malicious conduct complaints.

1.3.2.3. Develop contract language and/or advisories that clarify the language of RAA Section 3.7.7.3, including the definition of “reasonable evidence of actionable harm” with input from registrars and non-contracted parties.

1.3.2.4. The GNSO could discuss what forms of illegal malicious conduct and what standard of evidence should result in a requirement to reveal the contact information of customers of privacy or proxy services, consistent with procedures designed to respect any applicable protections for privacy and freedom of expression.

1.4 Additional Information on Registrars and their Affiliates

Statement of the Problem:

The recently adopted 2009 RAA includes additional requirements that apply to a Registrar's affiliates, resellers and proxy services. These include the following new terms: (a) RAA Section 3.11, that allows ICANN, under certain conditions, to terminate a registrar's accreditation in the event that one of its affiliates is in breach of its obligations to ICANN, and (b) RAA Section 3.12, that includes specific requirements for the reseller agreement and the registration agreements with the registrant, such as specific requirements related to consensus policies. Compliance with these new provisions would be facilitated by receipt of additional information from registrars regarding their ownership, their affiliates involved in domain name related services, their resellers, and the proxy services they provide or make available.

In addition, the law enforcement and the security community has been requesting ICANN to conduct additional inquiry on registrars, resellers, and proxy/privacy service providers that may be facilitating, enabling or are actively complicit in allowing malicious conduct to occur. For new gTLDs, ICANN has proposed a model of background checks and investigation of applicant registry operators that includes a vetting and verification process. It is reasonable that such solutions may be applied to registrars also.

Recommendation:

Additional Information regarding registrars, their affiliates and resellers will facilitate the identification of any actors that might be actively complicit in allowing malicious conduct to occur.

Implementation Options:

1. Insert a new section in the RAA requiring registrars to submit, on an annual basis, additional information to ICANN, for use in vetting and verifying the identity of the registrar and its affiliates. Such categories of information could include: additional details on the registrar's officers and directors (e.g., names, postal addresses and contact information); names, postal addresses and contact information of affiliated entities that engage in domain related services; the identity and ownership of registrar's parent corporations, if applicable; names, postal addresses and contact information for significant resellers (e.g. resellers registering more than 50,000 or 5% of its domain names under management); and names, postal addresses and contact information for any privacy/proxy services offered or made available by registrar or its affiliates.

2. In the event that ICANN receives information that a registrar, its affiliates, parent entity, officers or directors, resellers, privacy or proxy services are alleged to have engaged in illegal, fraudulent or malicious conduct, the registrar would agree to cooperate with ICANN in its investigation.
3. Include a new RAA Section 3.12.7 requiring resellers to provide and maintain complete and accurate contact information for a point of contact for malicious conduct, including allegations of fraud and domain name abuse (e.g., recommended by SSAC 38).

Category 2: Amendments to RAA to Improve Agreement Clarity and Promote Registrar Compliance with Existing RAA Obligations

2.1. WHOIS Inaccuracy Claims

Statement of Problem:

Current RAA Section 3.7.8 provides, that "Registrar shall, upon notification by any person of an inaccuracy in the contact information associated with a Registered Name sponsored by Registrar, take reasonable steps to investigate that claimed inaccuracy. In the event Registrar learns of inaccurate contact information associated with a Registered Name it sponsors, it shall take reasonable steps to correct that inaccuracy." <<http://www.icann.org/en/registrars/ra-agreement-21may09-en.htm#3.7.8>>

ICANN has issued advisories that attempt to explain and clarify this requirement to registrars <<http://www.icann.org/en/announcements/advisory-03apr03.htm>>, and <<http://www.icann.org/en/announcements/advisory-10may02.htm>>, but this continues to be a problem area in terms of clarity, compliance and public perception.

ICANN continues to receive many complaints about inaccurate and incomplete Whois data. The current RAA requires registrars to take "reasonable steps" to verify or correct Whois data in response to reported inaccuracies, but the RAA does not include a clear definition of the minimal required actions that registrars are expected to take.

Recommendation:

Incorporate additional terms in RAA requiring registrars to take reasonable steps to "verify" Registered Name Holder WHOIS data when inaccuracies are detected.

Implementation Options:

1. Clarify the existing registrar obligation to take reasonable steps to verify or correct Whois data in response to reported inaccuracies. At a minimum, "reasonable steps" to investigate a reported inaccuracy should include promptly transmitting to the registrant the "inquiries" concerning the accuracy of the data that are suggested by RAA Subsection 3.7.7.2. The inquiries should be conducted by any commercially practicable means available to the registrar: by telephone, e-mail, or postal mail. A registrar should also report to ICANN what action, if any, was taken in response to the reported inaccuracy. If the registrant has materially breached the registration agreement (by either failing to respond to registrar's

inquiries or by willfully providing inaccurate information), then the registrar should either suspend or delete the domain registration.

2. Adopt a Registrar Code of Conduct (RAA, Section 3.7.1) that incorporates provisions to achieve similar results.

2.2. Examination by ICANN of Registered Name Holder Registration Data

Statement of Problem:

RAA Section 3.4.3 requires a registrar to make records available for inspection and copying by ICANN upon reasonable notice. The overall efficiency of ICANN's compliance investigation processes will be enhanced by giving ICANN the option to request that registrar records be transmitted to ICANN via postal mail, courier, fax or email instead of simply being "made available" at the registrar's business office.

Recommendation:

Incorporate an additional requirement in RAA Section 3.4.3 requiring registrars to produce and send copies of records directly to ICANN when requested.

Implementation Options:

Amend the language of RAA Section 3.4.3 as follows: "During the Term of this Agreement and for three years thereafter, Registrar shall make these records available for inspection and copying by ICANN, or if requested by ICANN shall transmit to ICANN either electronically or by mail a copy any such records relating to a particular compliance investigation."

2.3. Termination of RAA by ICANN

Statement of Problem:

2.3.1 In recent months, ICANN observed two registrars who appeared to abandon their businesses. ICANN was successful in finding other RAA violations that allowed ICANN to terminate the registrars in those cases and transfer the data to a successor registrar. If, however, other grounds for termination were not present, ICANN would not have been able to take immediate action to protect registrants. When a registrar effectively abandons its business, registrants' domain name rights and domain name operations are severely impacted and ICANN should have the right to immediately terminate the RAA.

2.3.2 Certain registrars engage in repeated and willful business conduct that rises to the level of a "fundamental and material breach" of their obligations under the RAA. In these instances, a registrar relies on its right to cure repeated breaches within fifteen working days after ICANN gives the registrar notice of a breach. Registrars who intentionally or willfully abuse the "right to cure" provisions in the RAA harm registrants' domain name rights through this continuing questionable business conduct and effectively abuse the "right to cure" provisions granted to them under the RAA by ICANN.

Recommendation:

Incorporate two provisions in RAA Section 5.3 that establish ICANN's right to immediately terminate the RAA when a Registrar either: (1) abandons or ceases to conduct business as a registrar; or (2) repeatedly and willfully has been in fundamental and material breach of its obligations at least three times within any twelve month period.

Implementation Options:

2.3.1 Amend the language of RAA Section 5.3.7 to allow ICANN to immediately terminate a registrar's accreditation when it abandons its business as a registrar.

2.3.2 Insert a new RAA Section 5.3.8 as follows: "Registrar repeatedly and willfully has been in fundamental and material breach of its obligations at least three times within any twelve month period."

2.4. Business Dealings with Registered Name Holders

Statement of Problem:

A Registered Name Holder licensing use of a Registered Name accepts liability for harm caused by wrongful use of the Registered Name, unless it promptly discloses the current identity and contact information of the licensee to a party providing the Registered Name Holder reasonable evidence of actionable harm. The term “promptly” has been interpreted inconsistently. The period of time in which a Registered Name Holder has to disclose identity and contact information of the licensee should be clearly established in the RAA and accordingly in the registration agreement.

Recommendation:

Incorporate in RAA Section 3.7.7.3 a provision that clarifies the period of time in which a Registered Name Holder must disclose the current identity and contact information of a licensee when a Registered Name Holder does not intend to accept liability for harm caused by the wrongful use of a Registered Name.

Implementation Options:

Amend the language in RAA Section 3.7.7.3 as follows: “A Registered Name Holder licensing use of a Registered Name accepts liability for harm caused by wrongful use of the Registered Name, unless it promptly (i.e. within five business days) discloses the current contact information provided by the licensee and the identity of the licensee to a party providing the Registered Name Holder reasonable evidence of actionable harm.”

2.5. Manner of Establishment of New and Revised Specifications and Policies

Statement of Problem:

The GNSO Council recently changed the voting requirements necessary to support the establishment of Consensus Policies within ICANN. Since the current language of the RAA refers to a voting structure that is no longer applicable, the RAA should be updated to be consistent with the bicameral house structure identified in the Bylaws.

Recommendation:

Amend RAA Section 4.3.1 (b) to clarify that the demonstration of consensus requires a GNSO Council Supermajority vote instead of a two-thirds vote of the Council.

Implementation Options:

Amend the language in RAA Section 4.3.1 (b) as follows:

“(b) a recommendation, adopted by **a supermajority** vote **determined in accordance with the ICANN Bylaws** of the Council of the ICANN Supporting Organization to which the matter is delegated, that the specification or policy should be established, and”

2.6. Insurance

Statement of Problem:

RAA Section 3.10 requires a registrar to maintain Commercial General Liability (CGL) insurance to cover liabilities arising from registrar's business operations. Section II.A.3 of ICANN's Statement of Registrar Accreditation Policy (SRAP) http://www.icann.org/en/registrars/policy_statement.html states that ICANN's primary purpose in requiring a registrar to maintain insurance is to provide domain-name holders reasonable compensation for losses caused by the registrar's wrongful covered acts. According to various insurers' available information, a CGL policy includes three basic areas of coverage: bodily injury; property damage, personal and advertising injury; and medical payments coverage. The language of Section II.A.3 of the SRAP seems to indicate that professional liability type-coverage might be an appropriate form of coverage for a registrar to maintain.

Recommendation:

Revise the insurance coverage a registrar is required to maintain.

Implementation Options:

Amend RAA Section 3.10 to allow registrars to maintain appropriate (TBD) insurance coverage to protect domain-name holders against losses caused by the applicant's wrongful covered acts.

2.7. Arbitration

Statement of Problem:

RAA Section 5.6 requires three arbitrators. The process to select three arbitrators is time consuming and expensive for all parties. The parties may be better served by the selection or appointment of one arbitrator.

Currently, the RAA includes the following two statements: (1) "This Agreement may be terminated in circumstances described in Subsections 5.3.1 - 5.3.6 above only upon fifteen (15) days written notice to Registrar (in the case of Subsection 5.3.4 occurring after Registrar's failure to cure), with Registrar being given an opportunity during that time to initiate arbitration under Subsection 5.6 to determine the appropriateness of termination under this Agreement." (RAA, Section 5.3); and (2) "In the event Registrar initiates arbitration to contest the appropriateness of termination of this Agreement by ICANN or suspension of Registrar's ability to create new Registered Names or initiate inbound transfers of Registered Names under Section 2.1 above, Registrar may at the same time request that the arbitration panel stay the termination or suspension until the arbitration decision is rendered." (RAA, Section 5.6). These provisions have the effect of staying the termination until the arbitration panel has granted an ICANN request for specific performance and Registrar has failed to comply with such ruling.

Recommendation:

Amend the RAA to reduce the number of arbitrators from three to one.

Amend the RAA to clarify that even if a registrar initiates arbitration challenging termination of its RAA, no stay of termination shall be available if ICANN determines the registrar's conduct is harming registered name holders.

Amend the RAA to allow ICANN to terminate or suspend a registrar's accreditation if a stay has not been ordered within ten business days after the filing of the arbitration.

Implementation Options:

1. Insert the following language in RAA Section 5.6: "There shall be one arbitrator agreed by the parties from a list of AAA arbitrators, or if the parties cannot agree within fifteen calendar days of the AAA request that the parties designate an arbitrator, the AAA shall choose and appoint an arbitrator, paying due regard to the arbitrator's knowledge relating to the domain name system."

2. Add limiting language to the RAA making clear that a stay pending arbitration shall not be available if ICANN determines, in its sole discretion that the Registrar's conduct is harming registrants.
3. Add limiting language stating that unless the arbitrator grants a stay within ten business days of the filing of the arbitration, ICANN may terminate registrar or suspend registrar's accreditation.

2.8. Administration of Contracts

Statement of Problem:

Current practice requires registrars to sign and deliver multiple appendices with ICANN for each TLD that it intends to carry, as well as an appendix containing the terms of the trademark license for the ICANN logo. With over 800+ registrars and potentially hundreds or thousands of new registries in the future, requiring each registrar to sign a separate appendix for the right to sell new gTLDs creates unnecessary paperwork and introduces delays in the process. The administrative costs of managing and storing these documents can be avoided if this process is streamlined.

Recommendation:

Revise the RAA to streamline the procedure for adding accreditation in additional TLDs.

Implementation Options:

1. The trademark related license terms could be incorporated as a separate section within the body of the RAA, eliminating the need for a separate appendix.
2. The ability to add new gTLDs can be managed more efficiently. Rather than require the execution of individual appendices for each new gTLD, ICANN can create an electronic process that allows Registrars in good standing (i.e., not subject to an outstanding breach notice) to request the right to carry additional gTLDs, and ICANN will electronically submit the names to the registries of those registrars authorized by ICANN to carry their TLD. Any additional terms and conditions necessary for the TLD can be incorporated into the terms of the Registry-Registrar Agreement.

2.9. Privacy and Security of Registrant Account Records

Statement of Problem:

The unauthorized access to registrant account data maintained by registrars has resulted in malicious activity such as unauthorized changes to DNS records and redirection of traffic to a domain. When unauthorized access or a breach of privacy of registrant data has been discovered, a registrar currently has no obligation to notify ICANN and the affected registrants. The RAA should be amended to require timely notification to ICANN and the affected registrants in these circumstances.

Recommendation:

Amend the RAA to require a registrar to promptly notify: (1) ICANN of any security breaches affecting the registrar or any part of its systems; and (2) affected registrants when there is reasonable evidence of unauthorized access to their accounts.

Implementation Options:

Insert language in the RAA defining a *security breach* as “the unauthorized access to or disclosure of registrant account data”.

Insert language in the RAA requiring a registrar to promptly disclose, to ICANN and affected registrants, any security breach of registrar’s IT network affecting its domain management systems after the discovery or notification of a security breach.

Insert language in the RAA defining *promptly disclose* by the registrar as “action taken in the most expedient timeframe possible and without unreasonable delay”. Action(s) taken by a registrar should be consistent with the legitimate needs of law enforcement, as applicable, or any other measures a registrar determines are necessary to define the scope of the breach and restore the reasonable integrity of the data system.