

The Registration Infrastructure Safety Group Comments on the ICANN High Security Zone and Malicious Conduct Mitigation Programs

Contents

1. Introduction	1
2. Summary	2
3. Mitigating Malicious Conduct	2
3.1. Major concerns	2
3.2. Vetted registry operators	3
3.3. Require DNSSEC deployment	3
3.4. Prohibition on wild carding	3
3.5. Encourage removal of orphan glue records	4
3.6. Requirement for a thick WHOIS	4
3.7. Centralisation of zone file access	4
3.8. Documented registry level abuse contact and policies	5
3.9. Participation in an expedited registry security request process	5
4. High Security Zone Verification Programme	6
4.1. Programme concept	6
4.2. Topics	7
4.3. General IT and data security - controls, infrastructure, processes and policies.	7
4.4. Registry specific IT and data security	7
4.5. Registry service performance	8
4.6. Verification of registrant identity	8
4.7. Verification of entitlement	8
4.8. Authentication/assurance for the registrant/registrar interface	9
5. Recommendations	9
6. Conclusion	10

1. Introduction

RISG or The Registration Infrastructure Safety Group (RISG) is a global group of Internet-related organizations whose mission is to facilitate dialogue, affect change, and promulgate best practices to address Internet identity theft, especially phishing and malware distribution. RISG members and invited experts work together to improve Internet security, develop domain name industry best practices and share data to improve overall Internet user security. RISG is registry-focused and includes organizations with significant experience related to the policy, legal, and operational challenges related to domain name security. Current membership includes: Afilias (.INFO), AusRegistry (.AU), CNNIC (.CN), InternetNZ (.NZ), Neustar (.BIZ), Nominet (.UK) Public Interest Registry (.ORG), SIDN (.NL), VeriSign (.COM/.NET), GoDaddy, MarkMonitor, Network Solutions, Oversee.net, Melbourne IT, Cyveillance, Internet Identity, McAfee, Shinkuro, Symantec, plus Observer members from national law enforcement in the US and UK.

RISG has prepared this Comment on two elements of the Draft Application Guidebook (DAG), specifically:

1. The explanatory memorandum on Mitigating Malicious Conduct; and
2. The explanatory memorandum on A Model for a High Security Zone Verification Program.

We welcome the opportunity to provide this feedback, which has been produced and agreed by all members of RISG.

2. Summary

Although we applaud efforts to foster greater security in the domain space, we are unable to support some of the proposed solutions and implementation procedures put forth by the explanatory memoranda and can only support minor elements of them being included in the DAG. Overall, the ICANN security proposals appear to ignore established security protocols, fail to provide adequate implementation detail, and inappropriately broaden the scope of ICANN's security responsibilities.

The definition of security in the two memoranda is broad and confusing. For example, trademark abuse is wrongly identified as a security issue and the memoranda thus prescribe measures to protect Intellectual property when in fact it is a distinct issue from security. A more constructive definition would be malicious registration of domains affecting security and stability of the DNS. Further, the memoranda convey the impression that ICANN, intent on delivering greater security, has chosen to focus on registries because of the contractual control it has on that part of the market, rather than taking a holistic view of the chain of actors involved in malicious conduct.

It is the opinion of RISG that rather than creating new, complex, and repetitive requirements, ICANN should concentrate on a wider view that includes the participation of cross-industry groups that have already successfully implemented solutions for these same security concerns.

RISG offers the following list of specific objections:

1. The inclusion of several measures that are out of scope for ICANN's limited technical coordination role; ICANN's mission is the security and stability of the DNS. This does not extend to malicious uses of domain names;
2. The apparent disregard for the GNSO and wider policy processes within ICANN for the formulation of policy matters such as WHOIS implementation;
3. The inclusion of several measures that are not related to security, such as those intended to protect intellectual property. Intellectual property infringement should be addressed, but it is not a security issue;
4. The lack of empirical evidence, academic study or substantive explanation for many of the measures to demonstrate either efficacy or demand;
5. The lack of consideration of the legal issues of indemnification, current contractual requirements and enforcement of current contracts; and
6. The lack of consideration of the market impact; in particular, the impact on differentiated service offerings by registrars.

3. Mitigating Malicious Conduct

3.1. Major concerns

Whilst there are some of the proposed mitigation measures that RISG supports, we have several serious concerns with others and, most importantly, with the overall nature of this proposal:

1. A number of the proposed mitigation measures raised in the memoranda are already in active discussion within the GNSO yet no mention is made of those specific ongoing policy processes despite these memoranda clearly adopting one point of view from within that debate. This appears to unreasonably supersede those wider policy processes,

where differing views on the impact on security of certain proposed mitigation measures (such as thick WHOIS) are still unresolved;

2. No study of either efficacy or demand is presented that might justify the proposed mitigation measures. In our view some of the proposals have no evidence that they will improve security;
3. The proposed mitigation measures, by being so prescriptive, limit innovation within both registries and registrars, despite the overwhelming evidence that innovation within the market has solved many major problems, such as standardized provisioning interfaces;
4. The most hard-learned experiences of registries and registrars with respect to security for domains are ignored by creating a single, identical and narrow layer for security, when there should be multiple, independent and broad layers. This follows the principle of “genetic diversity”, which heavily influences the provision of root and TLD nameservers. A single layer creates a blueprint for bad actors to plan how to circumvent the controls.

We recommend that the proposed mitigation measures that are already the subject of GNSO discussions are so identified and any substantive discussion of them is removed and replaced with placeholders to the GNSO debate.

3.2. Vetted registry operators

We support this proposed mitigation measure in principle but note some concerns with the proposed implementation:

1. Rule ‘c’ that allows ICANN to deny anyone who – *“is currently involved in any judicial or regulatory proceeding that could result in ...”* is a rush to conclusion and ignores the possibility of false claims that may be remedied through legal process.
2. No mention is made of what happens in the event of a change of control of the registry, when this is clearly a point at which vetting may be circumvented if not repeated.
3. The opportunity exists to game the process by setting up multiple holding companies or use of agents.

We recommend the following:

- I. Inclusion of procedures for the Rule ‘c’ to also apply in the event of a “change of control” to mitigate circumvention of this rule at a later date.
- II. Prohibitions against gaming the Rule by setting up multiple holding companies or use of agents.

3.3. Require DNSSEC deployment

We support the deployment of DNSSEC but have concerns over the requirement for implementation by launch.

We recommend the following:

- i. That the requirement that new TLDs implement DNSSEC before or at launch be removed and replaced by one requiring implementation within an acceptable timeframe. That timeframe may depend upon issues raised in the recent root zone scaling studies.

3.4. Prohibition on wild carding

We support this proposed mitigation measure in principle.

We note that the ICANN board has already passed a resolution requiring prohibition on wild carding for all new gTLDs, though there remains uncertainty on how this is to be implemented in existing gTLDs.

3.5. Encourage removal of orphan glue records

This is a large topic, inadequately dealt with in either memorandum and should be a wider policy. The proposed mitigation measure can only have any effect for orphan name servers within the same registry, yet no evidence is presented as to the proportion of this problem that is within a single registry compared to across registries. Moving this topic into a wider policy discussion would enable discussion of the cross-registry implications, which may provide far greater security benefit.

We also note that the phrase “orphan glue records” is technically incorrect and the phrase “orphan name servers” is a correct description, as it is entirely possible to have orphan name servers without any “glue.”

We recommend the following:

- I. That this mitigation measure remain with an acknowledgement that it is only a partial solution to the problem, the other part being cross-registry “orphans”.
- II. That the topics that are worthy of wider policy discussion are raised in the appropriate open policy forums, with particular regard to the cross registry component and how that might be mitigated.

3.6. Requirement for a thick WHOIS

We support this proposed mitigation measure but note the following concerns with the proposal:

1. RISG recognises that better WHOIS data will help security mitigation by providing better access to data, but there is no clear evidence that provision of a thick WHOIS will lead to better quality of data, or that other measures will not prove more effective;
2. ICANN should not create a contractual right to impose unknown and arbitrary technical requirements on new registries. ICANN’s movement to alternative formats and protocols should be consistent with its consensus policy making and should not be imposed by ICANN in lieu of resolution of the ongoing WHOIS protocol considerations;
3. Because data is distributed in a thin WHOIS registry, this model requires cooperation and compliance with ICANN policies to ensure that all sharing parties provide legitimate users timely access to registration information. Some parties do not fulfil these obligations, either by restricting legitimate use or blocking access to WHOIS data entirely. ICANN’s response to non-compliant organizations has been uneven, and does not consistently result in restoration of access to shared WHOIS data.

We recommend the following:

- I. That ICANN review the impact of dealing with current failures within the thin WHOIS model as a quicker means of achieving some success.

3.7. Centralization of zone file access

There are differing views within RISG on the whether or not access to zone files improves security. For example, we note that many ccTLDs do not release zone files at all and some only under the strictest of conditions, because they regard open access to zones as a major security threat. On the other hand, many security companies regard access to zone files as absolutely necessary to combat e-crime. The same companies also make the point that

differing access methods make the task of obtaining zone files more complex than need be. But the counter argument is that making it easier for security companies also makes it easier for spammers or other bad actors, who would only need to falsify one application to get hold of all gTLD zone files.

This debate identifies the main issues, which are:

- who gets access to zone files;
- for what purpose they get access; and
- how they get access.

This proposed mitigation measure only looks at the last of those issues, bypassing debate of the bigger picture, and does not explore alternatives that might deliver a better solution. For example, looking only at the issue of access, there could be a central body that vets access and registers encryption keys that are then distributed to registries to enable secure zone transfer.

Furthermore, in the context in which it is presented, it appears to be directed more at intellectual property concerns than security concerns. Consequently, we cannot support the proposed mitigation measure.

We recommend the following:

- I. That this mitigation measure be removed until the outcome of a wider policy process.
- II. That the focus of this mitigation measure be rewritten to clearly identify it as a measure aimed at improving security, not protecting intellectual property.

3.8. Documented registry level abuse contact and policies

There are three parts to this proposed mitigation measure: the publication of abuse contacts; a vague discussion on mandated abuse handling policies; and the publication of abuse policies.

We are generally supportive of the publication of abuse contacts in principle, but note again that this should be the subject of a wider debate across all TLDs with consideration given to the abuse contact being included as part of the IANA database of TLDs and published in the IANA WHOIS. To that end we recommend that any substantive proposal is replaced with a placeholder to that discussion.

For the second part, mandated abuse handling policies, we do not regard it as within ICANN's purview to develop or mandate such policies. It is better for external bodies to bring together registries, registrars, security companies, law enforcement and others to look at and develop best practices for such problems across TLDs.

While ICANN clearly has a role to play in combating domain name abuse it does not extend to combating credit card fraud, identity theft, or many other problems that all have to be tackled by registries, registrars and other actors within the market.

For the third part, publication of abuse policies has little deterring effect.

We recommend the following:

- I. That this mitigation measure be removed.
- II. That the topics that are worthy of wider policy discussion are raised in the appropriate open policy forums.

3.9. Participation in an expedited registry security request process

RISG supports the concept of ICANN providing limited contractual compliance relief from certain registry duties so as to expedite response to critical security threats that require immediate action. However, ICANN needs to provide greater detail on the types of relief that will be provided, how such authority will be granted and the types of threats that will qualify for such relief.

We recommend the following:

- I. ICANN provide further proposals on:
 - a. The types of relief that will be provided.
 - b. How such authority will be granted.
 - c. The types of threats that will qualify for such relief.

4. High Security Zone Verification Program

4.1. Program Concept

We do not support the principle of ICANN running an extended verification program of this nature, because:

1. It is out of the scope of its role for ICANN to run such a program;
2. The program is fundamentally unable to assure the public of lack of malicious activity, as acknowledged in the memorandum; *“Due to the risks involved measures will be needed to limit liability to ICANN. If established, ensuring public awareness of the limitations of the program in terms of not providing guarantees about the presence of malicious activity within a TLD must also be addressed.”* Despite this it is proposed to issue a seal, as a mark of trust, for registrants to see at the time of purchase. A seal implies assurance especially if also targeted at the general public. If the seal is not able to do that fully, it will be seen as a marketing gimmick and therefore of little value. Furthermore, a seal may also impose legal and liability implications for ICANN which ICANN may not wish to assume;
3. The program will compete with multiple industry initiatives that are aiming to achieve the same goals but are doing so in an open and consensus based process that is therefore more likely to succeed;
4. The program exposes ICANN to unacceptable costs and liabilities without indemnifying any parties;
5. There are significant benefits to be gained from better enforcement by ICANN of current contractual obligations. Given the history of enforcement and compliance, it is difficult to predict success for the program;
6. A seal can be easily duplicated or reposted and the cost of monitoring and compliance to ICANN of proper usage will escalate with the number of new TLDs and the potential for misuse of the seal by registrars and their many resellers; and
7. A seal presumes the public is aware of what it means. An education campaign to educate the public about a seal is costly and time consuming and as the report itself admits, cannot guarantee the public will become more aware of malicious activity.

We recommend the following:

- I. That this program be dropped and the topics that are worthy of wider policy discussion are raised in the appropriate open policy forums. These topics are:
 - a. General IT and data security; and
 - b. Registry specific IT and data security.

4.2. Topics

While this program sets out a number of principles, examination of those principles shows a conflation of loosely related topics to create an artificial notion of a “high security zone”. In particular the principles confuse the two distinct objectives of a secure zone and a vetted zone. For the first, the operations of the registry are verified and for the second, registrants and their data are verified.

Once again, we make the point that the proper place for discussion and decision on many of these topics is the GNSO policy processes, where bottom-up policy is developed. Such policy, because of the wide involvement of interested parties, is generally much more sophisticated and detailed than the proposals here.

While some of these topics are appropriate, RISG has major concerns with others:

1. Some topics are out of scope for ICANN to be involved in;
2. Some topics are nothing to do with security; and
3. Some topics duplicate many procedures that are already common and can be voluntarily adopted.

Although the memorandum does not split out the topics, we have done so below in order to comment properly on them.

4.3. General IT and data security - controls, infrastructure, processes and policies.

This topic is introduced in the memorandum by inclusion of possible criteria topics such as:

- *1.1 Registry Infrastructure Security*
 - *Security management*
 - *Personnel security*
 - *Physical access control*
- *1.3 Confidentiality and Privacy of Sensitive Data*
 - *Data collection, use, retention, access and disclosure policies*

We do not support ICANN developing its own program for the assessment of IT and data security. This is already covered by an external quality standard such as ISO 17799, which was developed over many years, with the involvement of multiple parties and is applicable to registry/registrar business models. In addition there are lots of firms and auditors who are well versed with the procedures and who can perform the audit.

This standard is well known within the industry and costs for compliance and audit are well established and hence likely lower than the costs for an absolutely new set of requirements and audits.

4.4. Registry specific IT and data security

This topic is introduced in the memorandum by inclusion of possible criteria topics such as:

- *1.1 Registry IT Infrastructure Security*
 - *Name resolution service management controls*
 - *DNSSEC deployment plan*

This topic is worthy of wider consideration, but we note there is no logic in making these important security considerations voluntary rather than mandatory requirements of new TLDs.

Unlike the general IT security topic, this topic requires specialist assessors because the registry business is so specialised it requires some years to learn in depth. These skills and experience needed by these assessors are the same as needed to review the rest of a new

TLD application and so these requirements, if rolled into that process, could then be assessed within the same framework as just more criteria.

While there are many circumstances where special treatment of security is necessary, this is not one of them.

4.5. Registry service performance

This topic is introduced in the memorandum by inclusion of possible criteria topics such as:

- *1.2 Registry IT Infrastructure Availability*
 - *WHOIS service availability*
 - *WHOIS service performance level*
 - *WHOIS service response times*

We do not support this topic being part of any security program because it has nothing to do with security.

As an aside we note that ICANN is seemingly unaware that any comparative metrics for registry operations cannot be ubiquitous across all sizes of registry but must scale with the number of registrations. For example, with a TLD of 10,000 domains a registry only needs to be able to process 10 changes per minute but with 10,000,000 a registry needs to be able to process 10,000 changes per minute. ICANN has had several attempts at benchmarking but they have failed to establish scale-based metrics on each occasion.

4.6. Verification of registrant identity

This is out of scope for ICANN to mandate.

The requirements of this topic are unrealistic in their reliance on burdensome registration authentication requirements and disregard for registrar equal access contractual requirements that are contained in most registry agreements with ICANN.

Authentication of registrant information at time of registration is not feasible as the current Registry/Registrar business model depends upon the ability to perform nearly instant registrations of domain names. Performing extensive authentications of registrant information may significantly delay the registration process and create burdensome delay and complication with little evidence that such procedures will provide additional security.

The assumptions behind this topic are unrealistic. For example, the document says *"It also builds upon the assumption that Registrars will be required to perform procedures to authenticate the accuracy of Registrant information at the time of domain registration. This further assumes that (a) the Registries will be able to select through objective criteria, the Registrars that they do business with to those Registrars whose operations maintain an appropriate control structure from Registry to Registrant and that (b) Registries will structure their Registrar contracts to require implementation of specific controls required by the Program"*

We should also point out the obvious, which is that the identity used for registration may be fraudulent as already happens with phishing registrations. In these cases, identity verification already takes place as part of the credit card authorisation and yet has failed to prevent these registrations.

We must assume, by the inclusion of this topic, that ICANN has not adequately considered that inclusion would effectively suspend "equal access requirements" for registries that would volunteer to participate in this program.

4.7. Verification of entitlement

The Explanatory Memorandum states *"Other considerations, such as controls to address intellectual property concerns, could be added as components for future consideration in the*

lifecycle of the program.” Intellectual property infringement is not a security issue and should not be included in this proposed program.

We are very concerned that the above statement was included in this memorandum, even as a placeholder for future consideration. It undermines the whole intent of this memorandum as a means to increase security. ICANN must fully define and understand the parameters of “security” and not include issues that are wholly outside the role of ICANN or even the definition of DNS security.

4.8. Authentication/assurance for the registrant/registry interface

This is out of scope for ICANN.

The service features offered by a registrar are an important part of their differentiation within the market. Some registrars focus very heavily on security, whilst others tackle a different sector of the market.

This range of services works well because not all domains are equal, even within a single TLD. Some domains allow access to a web site used by millions, while others are virtually disposable.

We note that any registry that chose to mandate any specific security controls within registrars would fall afoul of the equal access requirements.

5. Recommendations

Our recommendations for the future of these proposals and the inclusion of these topics within the DAG are as follows:

1. For the malicious conduct memorandum:
 - a. To remove all reference to those proposals that are out of scope for ICANN;
 - b. To remove all reference to those proposals, such as IP protection, that are not related to security; and
 - c. For proposals that are currently the subject of an existing policy process, to put in a placeholder linking to that policy process with the determination on applicability to follow the outcome of the policy process.
2. For the high security zone verification program:
 - a. To remove the proposal for such a program. RISG believes this proposal is entirely out of scope of ICANN’s authority and, as currently proposed, is premature and lacking critical detail; and
 - b. To initiate a policy consultation process on the few elements that are within scope of ICANN and related to security, with a view to making them mandatory requirements for new TLDs.

We recommend that ICANN takes the following steps as alternatives to achieve the same objective of a more secure domain name market:

3. Thorough review, audit and enforcement of existing contractual requirements;
4. Provide greater reliance on existing standards and solutions that resolve the same concerns;
5. Move much of the debate away from focusing solely on registries and towards a wider view of the industry. Specific discussion points should include:

- a. Define where the baseline should be for security within registrars and the registrar/registrant interface; and
 - b. Greater choice for registrants, such as the possible creation of a high security registration.
6. Engage with cross-industry groups with the same level of commitment and resources as shown in the preparation of these memoranda.

6. Conclusion

RISG applauds ICANN's proposals to improve security, however we believe that these efforts, while well intended, are not the appropriate solutions for these concerns. RISG is primarily concerned that ICANN's proposals appear to ignore existing audit/security protocols, fail to provide adequate implementation detail, and inappropriately broaden the scope of ICANN's security responsibilities.

It is also the opinion of RISG that rather than creating new, complex, and repetitive requirements, that ICANN should concentrate on a wider view that includes the participation of cross-industry groups that have already successfully implemented solutions for these same security concerns. ICANN must also exercise greater care not to supersede the policy development process and to be more cognizant of its limited technical coordination role.

Lastly, prior to implementing any new security requirements, ICANN should provide empirical data to demonstrate market demand, need, and the impact of such new requirements.