SUMMARY OF THE NINE SAFEGUARDS (AGAINST DNS ABUSE) REPORT

# Introduction

The safeguards against DNS abuse report was published on the 18th of July 2016 and the document is structured around six (06) sections as follow:

1. Introductory remark
2. DNS Abuse key terminology
3. DNS stats and trends
4. Presentation of the proposed nine safeguards to mitigate DNS abuse
5. Research proposal and model to measure effectiveness of the safeguards and
6. Conclusion

According to Section 9.3 of ICANN Affirmation of Commitments to promote competition, consumer choice, and consumer trust in the Domain Name System (DNS) this report intends to help the review team by:

* Providing an overview of the state of DNS abuse following the roll-out of the New Generic Top-Level Domain (gTLD) Program in January 2012
* Discussing options for measuring the effectiveness of the nine safeguards put in place to mitigate DNS abuse in new gTLDs
* Proposing a research model to help assess the effectiveness of the nine safeguards in mitigating DNS abuse in new gTLDs

The objective is to examine the impacts of the new gTLDs – as a result of the expansion[[1]](#footnote-1) – on consumer choice, consumer trust, competition and the effectiveness of the nine safeguards techniques put in place to mitigate DNS abuse, which is the main focus of the work of the review team. Therefore, the report was organized to, firstly, present an in-depth examination of each of these safeguards, then, propose potential means to measure their effectiveness where possible, and, finally, put forward a research model to analyze their effectiveness in a rigorous and comprehensive manner. The nine safeguards are answers to four critical questions related to DNS abuse, and for each question, background on the safeguard method, its effectiveness, context and possible methods for data collection are discussed.

# Terminology

According to the report, DNS abuse covers a wide range of activities including – but not limited to cybercrime, hacking, etc. However, ICANN has defined, in the past DNS abuse as any activity that can be seen as “Malicious Misconduct”[[2]](#footnote-2).

## Tactics and Instruments

Bad actors mostly carry out their actions through compromised domains, malicious registrations, subdomains resellers, IP addresses (phishing) or shortened URLs. DNS abuse attacks can take any form but the typical aim is to distribute malwares.

The Registration Abuse Polices Working Group (RAPWG) developed a consensus definition of the work abuse within the distinction between two cases of it: during “registration” and “use”, and as a consequence, two categories of activities fall under DNS abuse.

# The Nine Safeguards

The nine safeguards intend to answer the following questions:

1. **How do we ensure that bad actors do not run Registries?**
   1. **Safeguard**: Vet Registry Operators. Effectiveness was measurable but preventiveness was not because no data exits to show how many applicants did not apply due to this safeguard.
2. **How do we ensure integrity and utility of registry information?**
3. **Safeguard**: Require Demonstrated Plan for DNSSEC Deployment: effectiveness on the 1st level (registry) was reached but no guaranty on the 2nd level TLD (registrars, DNS hosting providers, ISPs, etc.): Intellectual Property Constituency said that it is effective
4. **Safeguard**: Prohibition of Wildcarding: Intellectual Property Constituency said that it is effective
5. **Safeguard**: Removal of Orphan Glue Records: Intellectual Property Constituency said that it is effective
6. **How do we ensure more focused efforts on combating identified abuse?**
7. **Safeguard**: Requirement for Thick WHOIS records. **In their public comments on this report, the Intellectual Property Constituency and DotMusic noted the effectiveness of thick WHOIS records in helping to curtail intellectual property infringement and taking action against online piracy**
8. **Safeguard**: Centralization of Zone-File Access
9. **Safeguard**: Documented Registry- and Registrar- Level Abuse Contacts and Procedures: The International Trademark Association and Intellectual Property Constituency suggested assessing registry operators’ responsiveness to abuse claims received via this channel in their public comments on this report. But point of contacts are also abused by spammers.
10. **Safeguard**: Participation in an Expedited Registry Security Request Process (ERSR)
11. **How do we provide an enhanced control framework for TLDs with intrinsic potential for malicious conduct?**
12. **Safeguard**: Create a Draft Framework for a High Security Zone Verification Program (recommended but not mandatory)

# Research Proposal and Models

Although state-of-the art shows an increase of DNS abuse after the launch of the new gTLDs, there is no proof that it is a (proportioned) result of the increase of the gTLDs name space or due to the new gTLDs themselves[[3]](#footnote-3). Therefore, the big question to answer, when analyzing the effectiveness of the nine safeguards, is:

**To what extent can the safeguards put in place to mitigate DNS abuse in new gTLDs account for the rate of abusive behavior in the DNS?**

To do so, this report proposes “a hypothesis-driven causal analysis” to test the relationship between these nine safeguards and the occurrence of abusive behavior in the DNS. The analysis uses both qualitative and quantitative methods and alternate solutions (user feedback interviews, focus groups, etc.) where it is not possible or easy to collect data.

Following the proposal and the models suggested in the report, it is now up to the CCT-RT to decide what is interesting for their examination of DNS abuse mitigation.

The authors of the report suggested to design a reference model for establishing a baseline on what data to use and how to use it, using a five-steps process:

1. Identify the research problem clearly. What is the empirical puzzle we’re trying to solve?
2. Review and synthesize previously published literature associated with the problem.
3. Clearly and explicitly specify research questions and/or hypotheses central to the research problem.
4. Effectively describe the data necessary to adequately answer the research questions and/or test the hypotheses, and explain how such data will be obtained.
5. Describe the methods of analysis to be applied to the data in determining whether or not the hypotheses are true or false.

Going through those steps will contextualize the analysis of the DNS abuse issue for the purpose of this report and establish a theoretical base model claiming that “**the introduction of safeguards to prevent DNS abuse in new gTLDs should result in a cleaner DNS space compared to the “legacy” TLD era when such safeguards did not exist**.”

Three testable hypothetical scenarios derive from the suggested base model:

* **Model 1:** The expansion of the DNS has resulted in a proportional decrease in DNS abuse 🡪 **Effective Safeguard Hypothesis.**
* **Model 2:** The expansion of the DNS via the New gTLD Program has resulted in a proportional increase in DNS abuse 🡪 **Ineffective Safeguard Hypothesis.**
* **Model 3:** The expansion of the DNS has had a null effect on DNS abuse 🡪 Ineffective **Safeguard Hypothesis.**

1. “New TLD domains are more than twice as likely as legacy TLDs to appear on a domain blacklist—a list of domains of known spammers— within their first month of registration.” Said some Researchers from the University of California, San Diego. (Bad actors are testing the new / increased domain space, there is more competition due to price drop, etc.) However, no effective conclusion can be drawn since there is “limited comparative evidence” because the new gTLDs have just been introduced. Comparative studies are to be conducted when enough data is available. [↑](#footnote-ref-1)
2. This is a working definition intended to serve as a baseline for the rest of the report and all safeguards should be assessed against this definition while case per case analysis can be driven. Also, it is important to point out that differences in jurisdiction may cause confusions and a great care needs to be taken so that a common understanding is used during evaluation of the effectiveness. [↑](#footnote-ref-2)
3. Important questions remain as to whether the New gTLD Program has contributed to an increase in DNS abuse that is proportional to the increase in the size of the DNS as a result of the Program, and— crucially—whether the safeguards put in place to mitigate it have been effective in achieving their intended objectives. [↑](#footnote-ref-3)