STAFF REPORT OF PUBLIC INPUT PROCEEDING

Publication Date:	01 February 2019
Prepared By:	ICANN Security, Stability, and Resiliency (SSR) team

Public Input Proceeding	
Open Date:	20 July 2018
Close Date:	24 August 2018

Important Information Links
Announcement
Public Input Proceeding
View Comments Submitted

Staff Contact:	Samaneh Tajalizadehkhoob	**Email:**	samaneh.tajali@icann.org

Section I: General Overview and Next Steps

This document is a summary of the input to, and responses from, the Office of the Chief Technology Officer Security, Stability, and Resiliency (OCTO-SSR) team on the independent comments of the Domain Abuse Activity Reporting (DAAR) methodology and reviews. The findings and recommendations from the reviewers and parties who provided comment will be considered in the final drafting of the methodology paper.

Note: For ICANN community familiarity this document uses the format of the public comment summary. The submissions provided, however, were in response to a call for public input, which is used for non-Policy Development Process input and allows for anonymous contributions.

Section II: Contributors

At the time this report was prepared, a total of 5 community submissions had been sent to the DAAR Public Input email address. The contributors, both individuals and organizations/groups, are listed below in chronological order by posting date with initials noted.

Organizations and Groups:

Name	Submitted by	Initials
Registries Stakeholder Group Statement	Samantha Demetriou	RySG

Individuals:

Name	Affiliation (if provided)	Initials
Paul Vixie	Farsight Security	PV
Derek Smythe	Artists Against 419 (aa419)	DS
Anonymous-1		A1
Anonymous-2		A2

Section III: Summary of Comments

General Disclaimer: This section intends to summarize broadly and comprehensively the submissions to this public input proceeding but does not address every specific position stated by each contributor. The preparer recommends that readers interested in specific aspects of any of the summarized submissions, or the full context of others, refer directly to the specific contributions at the link referenced above (View inputs Submitted).

DAAR Objectives

1- **A1:** “DAAR supports science, in that it supports ‘structured observations of the empirical world.’ In general, blacklist curation seems to be science in this sense. Current anti-abuse work can be seen as essentially forensics --- not in the narrow sense of "digital forensics" but in the broader sense of applying scientific methods to provide evidence about a crime (or, in our case, a policy violation, which is conceptually the same thing). Supporting studies is one of the purposes you list, so perhaps the arguments in this paper might help make that link more explicit? This might be background, not foreground, argument.”

2- **RySG:** “ICANN Org has so far failed to justify its reason for creating DAAR. It is still a solution in search of a problem.”

3- **RySG:** “The DAAR may prove to be a highly useful tool for researchers to utilize, but ICANN Org has not yet justified to the ICANN Community why it spent the money to build a secret tool for which it now seeks post hoc approval and endorsement.”
RySG: “The RySG objects to and has grave concerns about both the lack of transparency about when and why ICANN chose to build DAAR and why ICANN continues to hunt for legitimate use cases. These are answers experts cannot provide. They can only validate after the fact “how” DAAR was built.”

4- **RySG:** “The statement of work makes it clear that ICANN has only partially understood RySG concerns about the feeds selected for DAAR and the inclusion of spam.”

5- **RySG:** “The ‘Purposes of the DAAR System’ (page 4) of the Methodology paper highlights a key concern that the RySG has with the DAAR initiative: Each of the purposes are couched in terminology that overtly suggests that DAAR can be of direct aid to the Registry Operator or Registrar in assisting with anti-abuse investigations. While DAAR outputs may be capable of indicating a likelihood or a trend of potential abuse, the system does not provide actionable evidence of that abuse. DAAR outputs are merely indicators, and not specific enough to enable a registry or registrar to pinpoint abuse, which would be essential in order for it to aid in any anti-abuse investigations that registries conduct, as the ‘Purposes’ section appears to claim.”
RySG: “The paper notes that the DAAR does not attempt to measure mitigation activity or otherwise provide tools for registries and registrars to address or resolve instances of abuse. The results are also only accessible by ICANN staff. As such, we have some concerns about the potential utility of this initiative, especially given the resources that have been devoted to developing it.”
A2: “In line with the abuse, we need to ensure that Bullet Proof hosting needs to be identified as one of the areas of abuse online. They are black hosting that service without any issues of the hosting organization and are never questioned and represent a large scale of the underground dark web. Most spam and porn etc., support. These are cloud equivalent support to all the main attacks and heavy users of IPs as well as hidden proxy services. We need a developed framework to approach the real trouble.”

6- **RySG:** “Bambenek, like Ranum, alludes to the future availability of DAAR as a research tool. This further alarms the RySG for the aforementioned reasons, as they heavily imply that ICANN has made commitments to provide researchers with access to the DAAR in the future, without providing any information or details to contracted parties or the rest of the ICANN community.”
RySG: “Has ICANN promised to make DAAR or its data available as a tool to researchers?”

7- **RySG:** “Bambenek says multiple times that ‘Not all abuse can directly be attributed to decisions made by registries or registrars.’ He then points to ways ICANN can mitigate the results and interpret the data to take into account which actions are attributable to contracted party actions (see pages 24 & 25 and page 34). We urge ICANN to explicitly agree with Bambenek's statement and carefully review Bambenek's suggestions.”
RySG: “Bambenek also says that ‘...making determinations in a programmatic way on whether a specific indicator is truly malicious, compromised, or simply a service provider being used by a criminal is well beyond the scope of DAAR’ (see page 4). This goes to the heart of our concern and we urge ICANN to understand that even if ICANN Org itself does not intend to use the data against registries, other people will.”

8- **RySG:** “The Registry Agreement currently requires registries to monitor for abuse. Before launching the DAAR initiative, we ask that ICANN demonstrate, with empirical data, that the majority of us are not doing this. Otherwise, it raises the question, what gap is ICANN trying to fill with DAAR?”

9- **DS:** “DAAR does not attempt to measure mitigation activity, i.e. it is not intended to measure how various parties (including registries and registrars) respond to abuse activity. This is a pity. However, we understand why this is extremely complex, encountering some of the obstacles ourselves. We attempt to monitor malicious domains checking statuses at least once per week. Registry rate limiting, and count blocking frustrates such attempts to a degree, especially where a registry or registrar has allowed an inordinate number of malicious domains into a registry, typically after a discounted domain price sale. The effect of such processing is felt for quite a while. Yet even so, such a full domain life cycle study does yield interesting results such as UDRP transfers and secondary abuse cropping up from time to time in the domain resales market.”

DAAR Aggregates Statistics

10- **PV:** "'Abuse scoring will be normalized and thus it will be more difficult for consumers of the report to deduce individual registries or registrars.' That makes DAAR less useful, bordering on academic. please reconsider. We must have a wall of shame; no icann-oriented process of review can be fast enough or adaptive enough to provide business risk to badly behaving registrars. Spamhaus reports on registries but lacks fine-grained sponsoring-registrar data and thus cannot report on registrars."
RySG: "Ranum says, '...DAAR is not 'naming and shaming' anyone…' He is correct in that DAAR, as a piece of technology, does not name or shame anyone. DAAR itself is agnostic. However, we know from experience how ICANN and other parts of the community can react to misinterpreted information and we are not confident that this data will be used to help registries."

11- **RySG:** "The DAAR does not provide aggregate statistics over individual RBLs, which prevents registries and registrars from identifying the lists that flag the most problematic domains and, by extension, addressing the underlying issues. Because the RBLs used have little overlap, registries or registrars seeking to act on these accusations have no recourse but to subscribe to the same set of RBLs (at least for particular security concerns) and build a similar DAAR system to identify accused bad actors. It is not clear what corrective steps registries and registrars might take, either to assist in clearing the good name of their customers or to restrict bad actors' usage of their systems."

12- **RySG: "**Relying on aggregate statistics also creates a risk of gaming the system by adding abuse domains from one's competitor registries or registrars to the RBLs used. The paper lists various disincentives against adding abuse, e.g., cost, discovery of bad actors, but if these disincentives were truly reliable, then the DAAR would not be necessary. In addition, damaging competitors' DAAR scores and reputations can also be accomplished by reporting additional domains (legitimate or not) from one's competitors to RBLs."

13- **RySG:** "The paper also fails to address the matter of miscounting domain names that may have been legitimately sink holed by law enforcement or security practitioners. Such domains have the potential to skew overall counts and thus the results displayed in the DAAR reports."

14- **RySG:** "Bambenek partially identifies, then discounts, a key RySG concern at page 31: 'The biggest risk is for small TLDs or registrars, but it is not likely this will be much of an issue....' Reputation is all many of us have to differentiate ourselves from our competitors. Furthermore, even large companies can be reputationally crippled by a single instance of inaccurate negative data. In today's fast-moving media, a hard-won reputation can be lost in an instant with no regard for the veracity of the claim. This risk is even greater for those registries and registrars that are or are Affiliates of publicly traded companies."

Use of Abuse Data Sources

15- **DK:** "Many Advance Fee Fraud (AFF) domains such as spoofs are inadvertently listed as phishing (and mitigated as such using incorrect methods). For these reasons, the statistics the DAAR system reports should be considered as a subset of the abuse problem in a given gTLD, or in the gTLD portfolio of a given registrar. It is our opinion that AFF should be considered as an additional category as the existing categories does not reflect the real consumer threat landscape. It's not uncommon, upon comparing notes with other parties to identify recurring areas of concern, but then notably areas where different operator at various levels appear based upon the type of abuse and the operator's recognition of such abuse."
RySG: "The ICANN community does not have a common, agreed-upon understanding of domain abuse overall, which raises the question of whether the DAAR initiative can really achieve the lofty goals laid out in the introduction to the paper. The DAAR initiative focuses on certain types of abuse related to domain names, e.g., phishing, malware, botnet command-and-control, and spam. While these are certainly serious issues that merit attention, they are not the only forms of abuse that impact domain names. In the past, the ICANN community has raised concerns over and worked to address other types of abuse like domain tasting and front running, which the DAAR initiative does not cover."
RySG: "Ranum says, '...if one is arguing against spam blocking, one is arguing for spam...,' which fallacy requires no explanation. The RySG of course opposes spam. What the RySG challenges is both its own role, and ICANN's, in lumping spam in with security threats because it crosses the line into evaluating content, which ICANN cannot regulate under its current Bylaws. We are not – and should not be – contractually obligated to monitor for spam and we're now being evaluated against a system that includes it."

16- **RySG:** "It is unclear whether an appropriate review has been conducted of how DAAR fits into ICANN's narrow remit as defined in the Bylaws. Security threats that relate to content and don't directly impact the DNS are likely out of scope for ICANN and the list of reputation data feeds should be reviewed against these criteria."

17- **RySG:** "The RySG has previously made clear statements expressing our concerns about the use of Spamhaus2, but ICANN has chosen to continue to use this source for the DAAR initiative. The RySG has significant concerns about the methods and practices Spamhaus uses, such as adding registrar infrastructure like SRS and mail servers to its RBLs, which could create security and stability issues."

18- **RySG: "**While the RySG appreciates Bambenek's thoughtful review of which blocklists ICANN should purge from its Malware Patrol feed and recommends ICANN accept this suggestion, as well as his careful review of the feeds to identify which ones may be content-based, we are concerned that he fails to review the five other 'major' sources. He seems to simply accept that these feeds are useful and valid simply because they are widely used."
RySG: "'Any complaints about the RBL scoring are not ICANN's problem, they are the RBL providers', or the registrars [sic]' and says '...if there are charges of inaccuracy, they are deflected over to the maintainers and producers of the blacklists.' This illustrates a key problem for the RySG: ICANN has chosen RBLs but has left the contracted parties holding the bag if there are problems with the feeds. Blacklists may refuse to talk to us or to whitelist our

domains even if we take corrective action or decide after an investigation that there is no abuse under our respective policies."

19- **A1: "**See Brunton (2013) for social history of spam (Spam: A Shadow History of the Internet). Spam is 'the use of information technology infrastructure to exploit existing aggregations of human attention.' Note that 'exploit' is in there. Security violations are exploits. This provides yet another tie to spam as a security problem. All the technical security exploits conducted by spammers as a result of exploiting human attention are well documented by Ranum and Bambenek and the DAAR paper. There's a good review of the Brunton book here: https://goo.gl/WMqTuF. There's some other good social arguments to pile on, perhaps: 'The principal effect of 'making spam scientific,' argues Brunton, was that the business of spam was left […] to the criminals.'"

Limitations in Abuse Data Sources

20- **A1:** "Constructively, consider building a small array of information about each domain, rather than simply presence or absence on a list. For example, note subdomain present, precise domain present, URL containing domain present. Perhaps subdomain contained in URL is an additional one that's useful. When the RBL maintainers make these more precise claims (subdomain, URL, etc.) rather than list an effective second level domain (eSLD), it's on purpose. I would suggest maintaining a hint of that information. Maintaining counts of unique subdomains and URLs on an eSLD is probably too complex. But a small three- or four-bit array for presence of different related parts (subdomain, URL, etc) seems doable."

21- **RySG:** "While the paper emphasizes the quality of the RBLs that the DAAR system relies on and asserts that they have low rates of false positives, the fact is that the DAAR system has the potential to amplify the negative effects of RBLs. Although these RBLs may have 'well-defined' processes for removing false positive domains, real-world experience has shown that 'well-defined' does not mean 'well-supported' or 'well-used.' In Marcus Ranum's review, he points out that this is not the DAAR's problem: it is an issue between the RBL and the domain registrant. The DAAR, however, is amplifying and anonymizing the RBL's potential mistakes in an unaccountable fashion."

WHOIS

22- **PV:** "The immediate impact of the DAAR methodology report is to enter into public evidence the following quite damning fact: 'A Whois query is the only means available to obtain the identity of a domain name's sponsoring registrar.' This was an accident of history, overlooked during the IFWP process which separated registrar functions from registry functions for the first time. We needed a machine-readable way to determine, at scale, the identity of the sponsoring registrar for a domain. By 'at scale' I mean that hundreds of millions of us needed and still need to determine the identity of a domain's sponsoring registrar, in a way performant enough to use this identity as part of the acceptance criteria for transactions. The absence of such a facility has allowed many registrars to operate in a very dirty, ugly, extractive, and public-abusive way. It's common to register domains and then drag one's feet about complaints. There is no business risk to a registrar who behaves in this way. In the absence of such business risk, these public-abusive behaviors have scaled quite well and that's a problem."

23- **RySG:** "The Methodology paper acknowledges that rate limiting sometimes makes gathering data very difficult but does not explain why real-time queries are necessary. Many registries and registrars have WHOIS terms of service that expressly prohibit automated, high-volume queries as the DAAR methodology describes using. Further, the paper states this challenge but does not provide any suggestions to work around it. Registries provide ICANN with access to bulk registration data files, but the paper does not consider this mechanism and why it may not be sufficient to meet the DAAR's needs. It also does not provide a strategy for how often to query to deal with transfers or updates."

24- **RySG:** "We have some concerns about whether the practice of having the DAAR collection system query registration data is compliant with GDPR and other privacy regulations. Such queries would require a disclosure of personal data that has not previously been contemplated and could have significant repercussions for both registry operators and ICANN."
A1: "Perhaps worth making it explicit that this project's relationship to GDPR? I don't think it's a big problem. But clearing these hurdles explicitly now that GDPR is in force may be wise?"

DAAR Project Communication

25- **RySG:** "We are disappointed that ICANN did not publish the DAAR methodology paper and attendant reviews through the standard public comment process. Many RySG members missed the announcement about these materials when it was published. Furthermore, collecting comments through a single email address is not transparent and does not allow community members to review and respond to each other's input."

26- **RySG:** "ICANN should provide more information about how it selects the sources for the DAAR collection system, including selection criteria and how the quality of the sources is assessed and measured over time."

Miscellaneous

27- **RySG:** "Additionally, the Methodology paper suggests that ICANN Compliance may be assisted by DAAR in the case of complaints filed against a registry or registrar. Members of ICANN's Contractual Compliance staff are already on the record as noting that they cannot use the DAAR statistics in isolation as an enforcement tool. It would be a worrying precedent should ICANN Compliance actually use such data, in its current form, to ground any enforcement action, especially considering the stated lack of actionable evidence and the decision not to perform any actual quality review or verification of the Data Feeds (RBLs) in use. It is unclear whether an appropriate review has been conducted of how DAAR fits into ICANN's narrow remit as defined in the Bylaws."

28- **RySG:** "The RySG urges ICANN to completely disregard the Ranum Paper. It contains numerous condescending, conclusory statements that are not justified by a single reference or even a logical argument. Furthermore, it accurately characterizes many of our concerns by casting them aside as hyperbole."

Section IV: Analysis of Comments

General Disclaimer: This section intends to provide an analysis and evaluation of the submissions along with explanations regarding the basis for any recommendations provided within the analysis.

DAAR Objectives

1- **Response:** This is a constructive point and we will make sure to raise it explicitly.

2- **Response:** As previously indicated to the community in various presentations and write-ups about the DAAR project, the reasons for creating DAAR included (1) a response to requests from portions of the community; (2) providing an unbiased compendium of data that can allow for observation of specific security threat trends; and (3) to provide information to the community to facilitate policy discussion. For example, one of the problems DAAR works to address is to provide an unbiased source of statistics collected using an open and documented methodology, instead of statistics deriving from efforts to promote specific products or services.

3- **Response:** ICANN org believes that increasing visibility and understanding of how abuse within the domain name space is viewed from the outside falls within ICANN's limited remit. DAAR is an instance of a tool that provides insight into domain name abuse.
We have made efforts to keep the community informed by sharing information about DAAR development progress, data used, and methodology at numerous ICANN meetings and with individual SO/ACs, including an RySG conference call as far back as October 2016. In order to ensure reliable output, we will not be publishing registrar related data and analytics until we are able to collect comprehensive data and develop reliable metrics for registrar abuse. Registry related aggregate analytics however will be published soon in the form of monthly reports.

4- **Response:** We kindly request RySG's to provide more written information so that we can better understand RySG's concerns regarding DAAR data feeds and the inclusion of spam.

5- **Response:** DAAR collects historical information that indicates what domain names are being operationally blocked on the Internet because those names are considered harmful by common reputation providers. The data used by DAAR is seen by the network operations community, e.g., email providers, ISPs, website operators, etc., as a reliable indicator of where abuse related to TLDs exists, and in what concentrations. As the DAAR methodology documents which reputation providers and lists offered by those providers are being used, registry and registrar operators are able to independently consume or monitor those blocklists as part of their anti-abuse efforts. Since the data DAAR collects does not include why domain names have been listed in reputation provider feeds, it only indicates that problems may exist. Whether the listing is actionable by the registry or registrar depends on context. Additionally, the base gTLD registry contract requires registry operators to "periodically conduct a technical analysis to assess whether domains in the TLD are being used to perpetrate security threats, such as pharming, phishing, and malware." As the data aggregated by DAAR is collected periodically, registry and registrar operators may therefore evaluate whether DAAR data would be suited for use as part of such technical analyses. Finally, in the future and after discussion with the ICANN community, we intend to provide mechanisms that will make the aggregate DAAR data associated with individual registries and registrars available to those registries and registrars.
As "Bullet Proof hosting" is outside of ICANN's limited technical remit, there are no plans to incorporate collection of statistics related to that hosting within DAAR.

6- **Response:** ICANN has not made any commitments to provide DAAR or its data to researchers. There are still ongoing discussions about whether and how the data will be published on the ICANN Open Data Program, in cases where licensing permits. ICANN org also intends to publish monthly reports based on DAAR data including anonymized aggregates and making the DAAR data associated with individual registries and registrars available to those registries and registrars.

7- **Response:** DAAR aims to provide methodology and aggregated statistics that may allow registries and registrars to learn more about how their businesses are impacted by security threats and how their anti-abuse programs are working. We will look into this attribution distinction as a part of future research plans.

8- **Response:** ICANN's mission includes the security and stability of the domain space. It is therefore reasonable for data to be collected to help informed decision-making processes. The DAAR platform looks at data across the gTLD namespace potentially giving a wider view than that afforded to individual registry or registrar operators. ICANN org is unaware of an abuse monitoring system that provides this aggregation via a documented methodology untied to any product or service, making the data available to the wider community.

9- **Response:** We thank the reviewer for the informative comment. As you have pointed out, DAAR is not measuring mitigation activity, since its focus is only on where abuse exists. The topic of "Domain life cycles" where they pertain to abuse is indeed an interesting topic for future research. However, it is not yet clear that DAAR is the correct place to do this.

DAAR Aggregates Statistics

10- **Response:** The purpose of DAAR is not to "name and shame" but to inform policy discussion related to a subset of security threats and DNS abuse. For now, we are aiming at publishing monthly reports including anonymized aggregates relating to security DNS abuse and threats impacting registries and are working on providing similar aggregates for registrars. Since those aggregates do not generally include sufficient information to distinguish individual actors, it is difficult to imagine how the data can be misinterpreted as the RySG asserts will occur.

11- **Response:** How many domains are listed as abuse in what TLDs is often published publicly by blocklist providers themselves (see for example http://www.surbl.org/tld). DAAR publishes the list of RBLs used along with aggregate statistics for each abuse type. DAAR aims to act as a starting point and help the community to understand the concentration of each abuse type. How data such as that collected by DAAR can be used to monitor abuse and ultimately make improved anti-abuse decisions is an interesting area for continued discussions. ICANN org is committed to working with the community to further understand how DAAR can help in abuse monitoring processes.

12- **Response:** Although gaming the lists may be plausible, it is highly unlikely since many of the RBLs used in DAAR have systems in place to validate the reporting stats. Gaming would require an industry actor to buy significant numbers of domains from a competitor and then to use those domains to perpetrate online crimes that would be detected by the blocklist providers, thus getting those domains blocklisted in a sustained way and at a large enough scale.

13- **Response:** This matter is specific to botnet command and control names. The DAAR system has some provisions in place to account for sink holing: 1) Much sink holing takes place in certain registrar accounts designated specifically for such purposes. These include registrar accounts set up by registry operators to hold DGA domains and domains suspended as a result of court orders. These accounts are recognizable and can be seen easily within DAAR in discussions with registry operators. 2) Since those domains can be recognized, the ability exists to back them out of TLD counts if they significantly skew the statistics. 3) Some blocklist providers do not blocklist domains pointed to known sinkholes since they do not pose security threats. These domains are therefore not counted as abuse domains in DAAR. What that said, this is something that we will continuously monitor as we plan future studies.

14- **Response:** To provide a level playing field, DAAR provides ways to account for operator size, among other important factors. It's statistically not correct that a "single instance of inaccurate negative data", i.e., a single false-positive listing, would have an impact on the reputation of an operator. The data is normalized by the size of the operator in terms of resolved domains. In addition, although bigger organizations have a wider attack surface, they presumably have more infrastructure in place to deal with the attacks, in comparison to smaller organizations.

Use of Abuse Data Sources

15- **Response:** The DNS infrastructure abuse monitored by DAAR was identified by the Government Advisory Committee (GAC) Beijing Communiqué of 11 April 2013, which led to a requirement in the new gTLD contracts to periodically conduct a technical analysis of security threat concentrations.

16- **Response:** DAAR aims to help identify the concentration of abuse in gTLDs as observed by widely-used reputation blocklists rather than being a comprehensive list of abuse. DAAR only includes DNS-related abuse types that are considered important by the community and for which reliable data is available. Issues such as domain tasting, and front-running are not considered security threats that pose a risk to the security, stability or resiliency of the DNS. They are business and domain registration process abuse that are not relevant to DAAR. The ICANN community can discuss and agree on whether specific forms of abuse should be considered DNS abuse as such. We are continuously reviewing the DAAR data and can incorporate different sources based on the outcome of the relevant community discussions.

17- **Response:** DAAR does not involve "content" issues such as trademark infringement, and the data feeds used do not involve such criteria. We intend to continuously review the feeds and exclude data related to content, as pointed out by the reviewers as well.

18- **Response:** DAAR will continue to review the best available data sources. Spamhaus' Domain Block List is among the most comprehensive abuse sources used in scientific studies published in top security venues. In addition, the listing of registrar infrastructure like SRS and mail servers is extremely rare and has no effect on DAAR scoring.

19- **Response:** DAAR simply reflects operational reality that can have an impact on the viability of registry's TLDs, whether or not DAAR exists**.** We are currently reviewing all the data feeds and will continue to review them on a regular basis in the future. We will take your concern into account when re-evaluating the blocklists. If specific blacklists are deemed problematic, appropriate actions, including discontinuing use of specific blocklists will be taken.

20- **Response:** This comment is well noted. We intend to make the definition of spam as a threat clearer in the DAAR methodology paper, as suggested by the reviewers

Limitations in Abuse Data Sources

21- **Response:** Thank you for this suggestion. We have to consider if such metrics fall within DAAR's scope, our licensing agreements, and how they add value to DAAR results. If and when in the future information in RBL data allows, we will further consider your suggestion.

22- **Response:** We respectfully disagree. The false-positive rates in the blocklists used in DAAR are extremely low; some exhibit a false-positive rate of about 0.1%, or one in a thousand. At such rates, false-positives do not affect the scores of TLDs and registrars in a meaningful way[123]. Further, DAAR's methodology is conservative by design. It favors operators by under-counting the lifetime of the threats. Domains that are listed for multiple issues are counted only once. In addition, the blocklists under-measure the abuse since they usually fail to identify a portion of abuse present on the Internet. Finally, the question of attribution of RBL to listing as well as RBL manual false positive checks in DAAR is something that we are currently working on.

WHOIS

23- **Response:** Indeed, the inability to associate names with registrars at scale is a limitation that we are aware of. It is our intention to look deeper into this problem space.

24- **Response:** The current agreement related to WHOIS collected in bulk does not allow for research access. Therefore, escrow files cannot be used for DAAR. In addition, the WHOIS

limitations affect registrar ID data only. Due to this limitation DAAR is not including registrar analytics data in its monthly reports and is currently limited to reporting on registries only.

25- **Response:** DAAR requires only the sponsoring registrar information, which is not personally identifiable information and poses no GDPR concern. Great care has been taken during the development of DAAR to ensure GDPR compliance. We continue to coordinate with ICANN Legal to ensure ongoing compliance.

DAAR Project Communication

26- **Response:** We are pleased that the RySG took advantage of the public input opportunity. ICANN org has more than one mechanism by which the community can provide input to the activities of the organization. The RySG refers to a process commonly used for policy development processes, contract modifications, and others. None of these fit the nature of DAAR. The choice of the methodology for the DAAR comment process allowed security practitioners to comment on DAAR in a way that protected their anonymity.

27- **Response:** We will include more details regarding selection methodology in the DAAR paper.

Miscellaneous

28- **Response:** Compliance will not be using DAAR data in isolation, rather it is merely one in a set of indicators that Compliance can make use of to identify potential areas of concern. During the audit, ICANN Contractual Compliance will review the registry operator security threat report and compare the data to publicly available abuse reports, including DAAR data. If ICANN determines that a report is incomplete based on this comparison, we will provide a sample of abusive domains from the publicly available reports that are not in the registry operator's reports. We will also provide evidence of each domain's abuse type, where applicable and available. Please see question #78 at this link https://www.icann.org/resources/pages/faqs-2012-10-31-en#DNS_Infrastructure_Abuse_Registry for more details.

29- **Response:** Both of the reviews were carried out in an independent manner. ICANN org feels that disregarding either review would be inappropriate. However, our aim is to further improve DAAR in terms of its data and methodology. Therefore, we welcome any input to help us reach that end.

[1] https://www.intra2net.com/en/support/antispam/index.php

[2] https://www.spamhaus.org/faq/section/Spamhaus%20SBL#8

[3] https://cseweb.ucsd.edu/~apitsill/papers/imc12.pdf