

Preliminary observations on responses to outreach by the GNSO Council Small Team on DNS Abuse

Third Presentation to the At-Large CPWG

Justine Chew

Member, GNSO Council Small Team on DNS Abuse

8 August 2022



Context for Outreach on DNS Abuse

- ⦿ Small Team of GNSO Councilors
- ⦿ Work assignment includes:
 - Outreach to ACs, SG/Cs, ICANN Contractual Compliance, DNS Abuse Institute (DNSAI)
 - Understanding landscape of DNS Abuse – which elements appear inadequately mitigated
 - Identify what might be in scope for GNSO policy making
 - Recommending to Council on next steps
- ⦿ Started prep in early Feb 2022; response review completed 4 Aug
- ⦿ **Preliminary observations; not final output**
- ⦿ Next step: Draft Report & Recommendations to GNSO Council



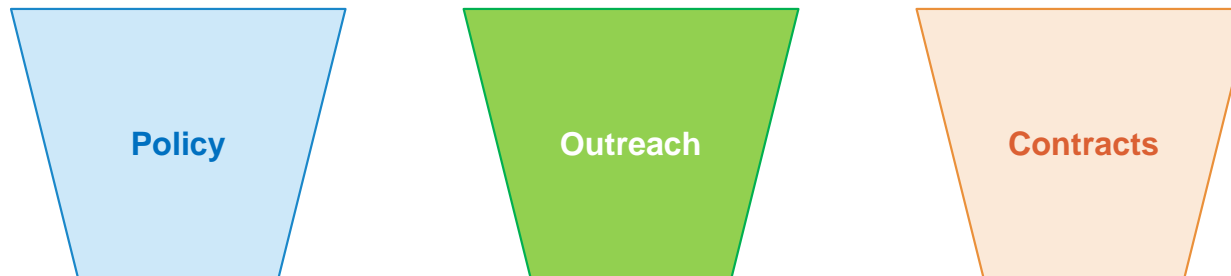
**High Level Approach
formulated by
GNSO Council Small Team**

High Level Approach with ACs, SG/Cs, DNSAI

⦿ Input sought

1. *What specific problem(s) would policy development in particular be expected to address and why*
2. *Expected outcomes if policy development would be undertaken*
3. *Expectations for GNSO Council onward undertaking in the context of policy development*

⦿ “3 Buckets” sorting





⦿ Recommendations pending

**PART 1: Preliminary Observations
by GNSO Council Small Team
of Responses from ACs
(as at 13 July 2022)**


Preliminary Observations by Council Small Team

⦿ ACs – ALAC (1/2)

Input	Preliminary Observations
<ul style="list-style-type: none">• Bulk registrations made with malicious intent such as used for botnet command & control, spam• Investigate methodologies to detect abusive behaviour, identify ways to vet/prohibit/reduce such bulk registrations, or make it financially unattractive• Eg of solutions cited:<ul style="list-style-type: none">○ Know Your Customer (KYC) should be applied to bulk registrations and registrants who do large number of registrations over time○ Predictive algorithms that identify potentially abusive domains at point of registration – Predator, Premadoma, ccTLD success cases with minimal false positives	<p>Issue 1: KYC potentially useful to prevent DNS Abuse</p> <ul style="list-style-type: none">• Do CPs practise KYC (for bulk registrations) across the board? How?• Potential overlap with other ICANN work and pending EU legislation on KYC• Basket: Outreach, for Policy much deeper analysis is necessary  <p>Issue 2: Are bulk registrations problematic?</p> <ul style="list-style-type: none">• Possibly but insufficient data to be sure, need further data on CP business practices in order to see if there might be a policy route.• Basket: N/A. Better for Council to facilitate community discussion to see if there is an issue <p>Issue 3: Use of innovative technology to prevent abuse</p> <ul style="list-style-type: none">• Basket: Outreach. Potential routes: <ul style="list-style-type: none">• A) OCTO to monitor, suggest use• B) Work with industry partners to socialize these tech• C) Webinars coordinated with ICANN Org to present tech to community

Preliminary Observations by Council Small Team

⦿ ACs – ALAC (2/2)

Input	Preliminary Observations
<ul style="list-style-type: none">• CP contractual obligations re DNS Abuse, eg Base Registry Agreement Spec 11 3 b – how well is Contractual Compliance using these to enforce compliance?• Registration data accuracy relevant to DN abuse<ul style="list-style-type: none">○ Incremental improvements○ Large-scale change to how registrations are managed○ Being considered by Accuracy Scoping Team• Use small team of experts + knowledgeable ICANN participants to more fully develop a catalogue of targeted activities, leading to Issue Report for possible multiple PDPs with strong representation from groups involved with cyber-security and active involvement from ICANN CC.	<p>Issue 4: Contractual Compliance’s effectiveness</p> <ul style="list-style-type: none">• From Contractual Compliance’s response to outreach, says:<ul style="list-style-type: none">○ “<i>have all the tools to do what they are tasked to do</i>”• RySG have acknowledged existence of “interpretation” – function of negotiation with ICANN Org• More transparency needed, to identify good faith efforts by CPs in interpreting contractual language to:<ul style="list-style-type: none">○ Help tighten “obligations” to acceptable min standard○ Help standardized “obligations” to apply to all CPs• Basket: yet TBD [Update: Contract – Letter to CPH]  <p>Issue 5: Registration Data Accuracy</p> <ul style="list-style-type: none">• Out of scope here.• Basket: N/A. <p>Issue 6: Expectation on next steps for Council</p> <ul style="list-style-type: none">• Recommendation pending (if any)



Preliminary Observations by Council Small Team

⦿ ACs - GAC

Input	Preliminary Observations
<ul style="list-style-type: none">• As the current community efforts focused on DNS Abuse are progressing, a PDP may be premature as long as such efforts continue to be fruitful• Ongoing community efforts may produce beneficial initiatives and outcomes not needing PDP.	<ul style="list-style-type: none">• PDP not the only option forward, need to explore all options and scope for each issue• Direct RySG/RrSG/ICANN negotiation could result in changes to all contracts applying to all TLDs but typically limited to very specific and clear issue already in contracts• Would GAC be interested in education side of issue?

Preliminary Observations by Council Small Team

⦿ ACs - SSAC

Input	Preliminary Observations
<ul style="list-style-type: none">• Refer to SAC115, consider to:<ol style="list-style-type: none">1. encourage standard definitions of abuse;2. encourage ‘notifier programs’ that will expedite and make more efficient abuse handling in certain parts of the ecosystem;3. determine the appropriate primary point of responsibility for abuse resolution;4. identify best practices for deployment of evidentiary standards;5. establish standardized escalation paths for abuse resolution;6. determine reasonable timeframes for action on abuse reports; and7. create a single point of contact determination whereby a reporter can identify the type of abuse and get directed to appropriate parties.	<p>Issue 1: Seamless environment for standardized reporting and parsing to right parties</p> <ul style="list-style-type: none">• DNSAI PIR’s sponsored tool (NetBeacon) is good example of approach, but it’s no contract-mandated and is run by 3rd party – its use would demand community consensus (but there are precedents)• Bucket: Policy / Outreach – possible to get ICANN to have own tool with enhanced methodology and more robust aggregation rules. <p></p> <p>Issue 2: Establishing clear timeframe, firm escalation paths, etc</p> <ul style="list-style-type: none">• Bucket: Contract / Policy – either through contractual negotiations or policy development <p></p>

**PART 2: Preliminary Observations
by GNSO Council Small Team
of Responses from SG/Cs & DNSAI
(as at 4 August 2022)**

Preliminary Observations by Council Small Team

⦿ Known, friendly, Third Party – DNS Abuse Institute

Input	Preliminary Observations
<ul style="list-style-type: none">• No need to fully and completely (re-)define DNS Abuse, start at the center, establish expertise and processes to mitigate malicious¹ registrations (i.e. unambiguous harm at core of DNS Abuse)<ul style="list-style-type: none">○ Malicious Registrations used for the distribution of Malware;○ Malicious Registrations used for Phishing;○ Malicious Registrations used for the operation of Botnet command and control systems• By limiting to malicious registrations, efforts stay within ICANN’s remit• Suggests to use series of narrowly-focussed PDPs to generate outputs that are short, simple, with easy to implement requirements – clear obligations for Rrs to mitigate malicious registrations which reflect existing industry best practices	<p>Issue 1: Scope/definition of DNS Abuse</p> <ul style="list-style-type: none">• Keep existing scope/definition: Malware, botnets, phishing, pharming, spam as vehicle – more or less established• Bucket: Policy / Outreach – with no need to derive new definitions; can build on existing work: Framework for RO to respond to identified security threats² <p>Issue 2: Malicious registration vs compromised domains</p> <ul style="list-style-type: none">• Bucket: Policy – distinction useful, not currently contemplated in ICANN contracts & policies, can build on existing work:<ul style="list-style-type: none">○ Maciej Korczyński’s “EC Study on Domain Name System Abuse”○ DNSAI’s “Malicious Registrations versus Compromised Website”¹ <p>Issue 3: Policy-making format</p> <ul style="list-style-type: none">• Bucket: Policy – narrowly-focussed, but requires balance between macro vs micro management
<p>1. Malicious registrations vs. compromised domains: see DNSAI Best Practice on Identifying Malicious Registrations [https://dnsabuseinstitute.org/best-practices-identification-mitigation-of-dns-abuse/]</p>	<p>2. See: Framework for Registry Operator to Respond to Security Threats, 2017 [https://www.icann.org/resources/pages/framework-registry-operator-respond-security-threats-2017-10-20-en]</p>



Preliminary Observations by Council Small Team

⦿ SGs – Registry SG (RySG) (1/2)

Input	Preliminary Observations
<ul style="list-style-type: none">• Believes “<i>there is room for both contractual requirements and best practices within industry both have a role to play in contributing to larger fight against DNS Abuse.</i>”• Supports setting minimum acceptable compliance standard – which ICANN community should seek to establish & ICANN Org to enforce<ul style="list-style-type: none">○ ICANN’s goal: to achieve such minimum compliance○ Must permit any RO to only achieve minimum compliance (as basic expectation) if chooses to do so• Support for minimum contractual standards in PD, yet equally supports industry efforts to – collectively or individually – elevate responses (practices), innovate beyond minimum expectation per ICANN contract<ul style="list-style-type: none">○ Expectations of a PDP must be tempered appropriately towards minimum compliance goal○ ICANN policy is necessarily separate from best practices –○ ‘Best practice’ has much broader concept and goal than base policy – not every such effort is suitable, or capable of being enshrined in ICANN policy immediately○ Such efforts should remain in purview of individual ROs, egged on by industry/RySG, leading to generally accepted practice (GAP) over time○ GAP = prime candidates for inclusion as min compliance standards	<ul style="list-style-type: none">• Noted that RA is not meant to combat abuse directly but rather managing the RZs, through use of certain tools (eg RBLs)• Noted that good actors within RySG are already doing due diligence but an elevated minimal standard could be beneficial to bring all actors to the same acceptable level• Consultation with Contractual Compliance had suggested possible gaps which could be addressed – there is a path towards better procedure• Need to avoid creating hard limits or a situation where external actors can exploit eg if 1,000 complaints logged, sanctions are taken• Need to take into account ICANN legal process in existing contractual negotiations• Consider having a small dedicated group to frame potential areas where more work can be done (for eg. on gaps gleaned from CC’s responses) – with flexibility in determining way forward

Preliminary Observations by Council Small Team



⦿ SGs – Registry SG (RySG) (2/2)

Input

- Having said above, RySG happy to partake in any PD work which is properly scoped, narrowly defined within ICANN's remit to achieve an implementable and enforceable outcome if stated issue
 - Goal being minimum compliance –
 - Through multiple discrete PDPs to support creation of policy aimed at universal, uniform solutions that only MSM can achieve to successfully produce new requirements in timely manner, supporting predictability
- Any proposed PDP (if Council so chooses) must:
 - Embed gating issue(s): proper scoping
 - Embed sufficient definition of issue(s) to be solved
 - Be predicated on realistic expectations – i.e.
 - [1] Creation of minimum acceptable policy (not creation of best practices); and
 - [2] Establishing minimum qualifying criteria
 - KIV that policy must support predictability – non-arbitrary and transparent



Preliminary Observations

Issue 1: Path forward?

- Bucket: Contract – step by step, starting with & build on what this exercise has established / collected 
- Letter to CPH (and ICANN Org?) suggesting:
 - Objective of expediting ability to combat DNS Abuse,
 - Seeking feedback on gaps identified from consultation with CC – that there is room for tighter focus in combat of abuse
 - Aiming towards contractual negotiations route first
- Bucket: Policy – as a possibility 

Preliminary Observations by Council Small Team

◎ SGs – Registrar SG (RrSG)

Input	Preliminary Observations
<ul style="list-style-type: none">• Thinks may be place for an ICANN-based agreement on DNS Abuse (as already defined) – to exclude concerns about content – for a limited-scope group, understanding the limitations of the DNS and applicable local laws, may help provide a global agreed upon response<ul style="list-style-type: none">○ Envisages a “Suggested Standards” document drafted by CPs in consultation with CC outlining:<ul style="list-style-type: none">[1] Standards for compliance (eg. standards for responses to abuse reports)[2] Situations in which CP recommend that CC take enforcement action (eg. consistent failure to address clear and actionable DNS Abuse)• Proposes a “registrant rights” document based on currently applicable policies – to clarify registrant’s right to demand a registrar investigate allegations of misuse of registrant’s DN<ul style="list-style-type: none">○ Result of a lack of communication rather than lack of action○ Helps inform/detail recommended actions of a CP, in turn helps CC efforts to enforce contracts as written	<h3>Issue 1: Path forward?</h3> <ul style="list-style-type: none">• Bucket: Contract – step by step, starting with & build on what this exercise has established / collected • Letter to CPH (and ICANN Org?) to include:<ul style="list-style-type: none">○ Objective of expediting ability to combat DNS Abuse,○ Seeking feedback on gaps identified from consultation with CC – that there is room for tighter focus in combat of abuse○ “Registrant rights” document may help clarify ICANN’s position on what “reasonable” means in RRA/RA, based on feedback from CC, seeking to address gaps○ Aiming towards contractual negotiations route first• Bucket: Policy – as a possibility 

Preliminary Observations by Council Small Team

⦿ SGs – NCSG

Input	Preliminary Observations
<ul style="list-style-type: none">• Does not believe there are any problems discussed in the community that require PD effort• Moreover, a common definition of DNS abuse which is in alignment with ICANN's bylaws and technical remit first needs to be adopted by the community• Expects next step is for such common community definition of DNS abuse	<ul style="list-style-type: none">• Does not recommend that matter of definition be the centre of discussion, there is a workable definition already• Instead recommends discussion be focused on outcomes

Preliminary Observations by Council Small Team

⦿ Cs – Business Constituency (BC)

Input	Preliminary Observations
<ul style="list-style-type: none">• Accepts that definitions of DNS Abuse already contractually defined, agreed upon by all relevant stakeholders• Able in most cases to differentiate between maliciously registered and compromised domain (but this is not in contracts)<ul style="list-style-type: none">○ Yet, malicious actors still able (in varying degrees of success) to register DNS maliciously, depending on which RO or Rr is selected – since action taken against abuse not uniform in scope or response time○ Belief that PD is needed to address this gap in non-uniformity (especially for clear-cut abuse cases eg malware distribution)• Use small, target PD that have short life cycles – don't attempt a PDP that seeks to solve every case observed but one that focuses on creating an environment in which actors have responsibility for quickly and efficiently reporting and addressing DNS Abuse:<ul style="list-style-type: none">○ [1] A sufficiently detailed complaint meeting “DNS Abuse” criteria should expect action taken within 24 hours of Locked and Suspended○ [2] ICANN Org should schedule periodic audits to assess obligation to respond to DNS Abuse reports – use test complaints to assess effectiveness of response and make this public information	<ul style="list-style-type: none">• Does not recommend that matter of definition be the centre of discussion, as multiple community actors have good routes to address that• Instead recommends discussion be focused on outcomes and practices that result from this distinction – “<i>what can effectively address the different needs and actions re: maliciously registered vs compromised DNSs?</i>” <p>Issue 1: Path forward?</p> <ul style="list-style-type: none">• Bucket: Policy, tentatively





Part 3: Responses from ICANN Contractual Compliance

Outreach on DNS Abuse with Contractual Compliance

⦿ Input Sought

1. *Overview of current requirements that CC enforces in relation to DNS abuse (ref: RA & RAA)*
2. *How enforcement takes place procedurally – resolving complaints and performing audits aside, how else does CC identify actionable information to investigate DNS abuse related complaints*
3. *Use of any metrics and/or trends for further insight into complaints*
4. *Factors taken into account when reviewing a complaint - consistently applied across board ('mandatory') vs. case-by-case basis ('discretionary') – what challenges in determining whether a CP is failing to comply - what would assist CC in making such a determination*
5. *Where CP determined as failing to comply – what challenges in effectively remediating non-compliance – what would assist to ensure effective remediation*

Response by Contractual Compliance (1)

⊙ Q1. CC enforces vide RA, RAA and others

Registry Agmt (RA)

Spec. 6, s. 4.1 – RO to publish accurate details - valid email, mailing address, primary contact for queries on malicious conduct in TLD

Spec. 11, s. 3(a) – RO-Ry contract must stipulate that in Rr-registrant contract registrant prohibited from engaging in certain activities – breach leads to suspension of DN

Spec. 11, s. 3(b) – RO to periodically conduct technical analysis to assess perpetration of security threats – pharming, phishing, malware, botnets – and maintain stat reports on numbers identified + actions taken

Spec. 4, s. 2 – RO to allow credentialed third-party access to zone file through agreement administered by a CZDA Provider (ICANN or ICANN designee [*requests normally submitted by security researchers who investigate and help combat DNS abuse*] – *impact of GDPR/Temp Spec?*)

Registrar Acc Agmt (RAA)

s. 3.18 – Rr required to:

- Take reasonable, prompt steps to investigate, respond to reports
- Review well-founded reports of Illegal Activity (per RAA) submitted by law enforcements, consumer protection, quasi-govt or other similar authorities within Rr's jurisdiction
- Publicly display abuse contact info, handling procedures

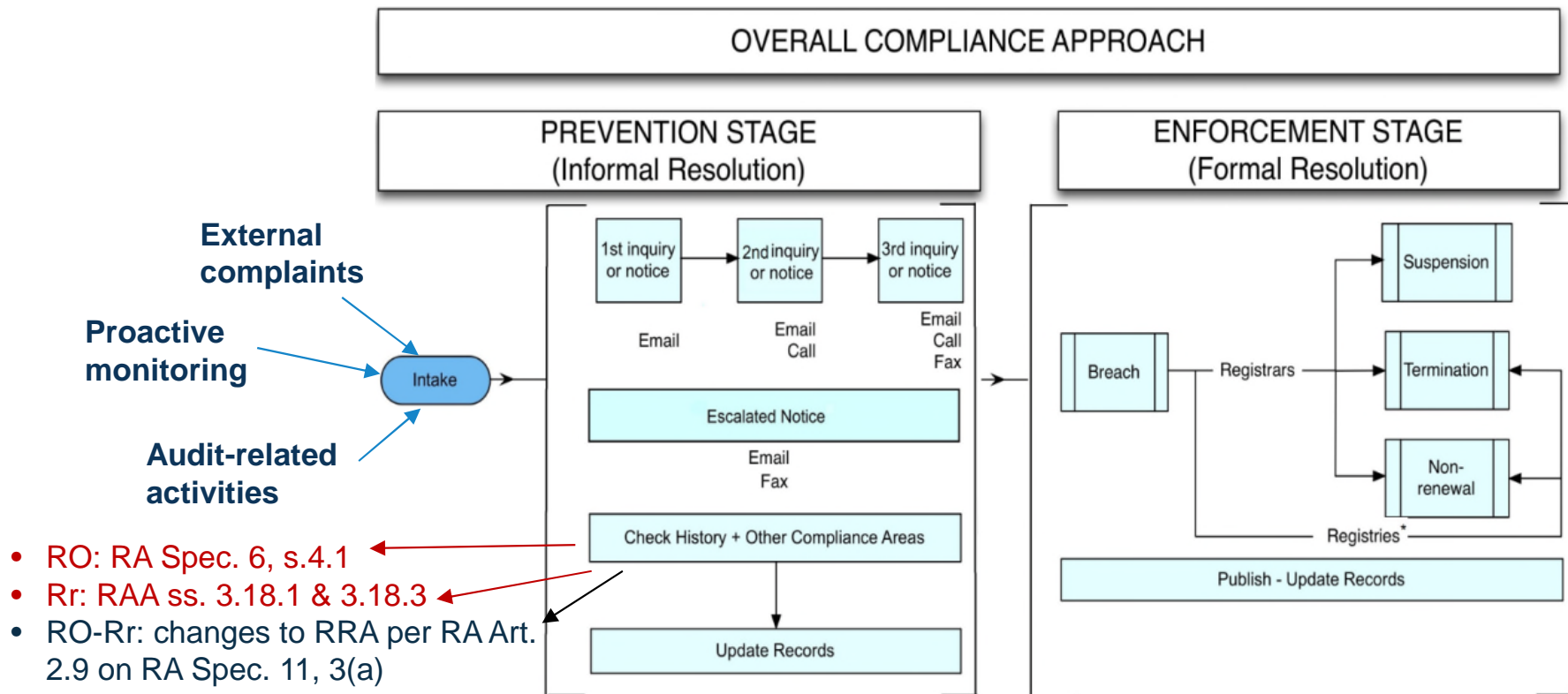
s. 3.7.8 – Rr to comply with obligations under Whois Accuracy Program Specification -- any Consensus Policy requiring reasonable and commercially practicable
(a) verification of contact info associated with a Registered Name sponsored by Registrar or
(b) periodic re-verification of such information.

Also to take reasonable steps to investigate claimed and correct inaccuracy.

Response by Contractual Compliance (2)

Q2. Enforcement Procedures using Established Process

- “ICANN Compliance enforces all obligations with its contracted parties through an established process which provides for a consistent and equal treatment approach.”
See: <https://www.icann.org/resources/pages/approach-processes-2012-02-25-en>
- Reactive and Proactive processes



- Formal enforcement notices are published: <https://www.icann.org/compliance/notices>

Response by Contractual Compliance (3)

⦿ Q3. Metrics/Trends on complaints investigated

- See: Dedicated Contractual Compliance reporting portal <https://features.icann.org/compliance> where 1st section “[Metrics and Dashboards](#)” provides monthly data
- Beginning in 2018, included subject matter category for Rr-related abuse complaints – spam, pharming, phishing, malware, botnets, counterfeiting, pharmaceutical, fraudulent and deceptive practices, trademark or copyright infringement, registrar abuse contact – as selected by processor in validating complaint by complainant
- Since 9 Mar 2022, publishing new tools – more granular data on complaints received, obligations enforced, and process for enforcement
 - See: <https://www.icann.org/en/blogs/details/new-icann-reporting-enhances-visibility-of-complaint-volumes-and-trends-09-03-2022-en>
 - Reports at: <https://features.icann.org/compliance/dashboard/trends-list>

Response by Contractual Compliance (4a+4b)

Q4. Factors taken into account in reviewing complaint

- Factors depend on details of complaint and the obligation(s) being enforced

Failure to Comply	Action	Note
RA Spec. 6, s. 4.1 – RO's failure to display abuse-related info	<ul style="list-style-type: none"> CC will review; if info is missing, deemed incomplete or inaccurate, RO required to remediate and provide evidence of remediation 	Mandatory obligation
RA Spec. 11, s. 3(a) – RO's failure to include provision on registrant prohibitions wrt certain activities	<ul style="list-style-type: none"> CC will request for provision to be included 	Mandatory obligation
RA Spec 11, s. 3(b) – RO's failure to conduct periodic technical analysis on security threats	<ul style="list-style-type: none"> The main focus in audit on RO processes, procedures re: prevention, identification and handling of DNS security threats Takes action per Compliance Approach 	Mandatory obligation. Found significant efforts by most ROs – 5% had been found non-compliant but remediated – Sep 2019
RAA s. 3.18 – Rr's failure to investigate, respond to reports / review well-founded reports of Illegal Activity (per RAA)/ publicly display abuse contact info, handling procedures	<ul style="list-style-type: none"> CC does not review whether reported DN is maliciously used Only validates if complainant submitted a fully formed complaint (+evidence) to Rr's abuse contact Validates compliance with RAA s. 3.18 – demonstration of compliance needed through itemized list of information requested Additional clarification, evidence sought if apparent discrepancy between action taken and Rr's own DN use / abuse policies. Until satisfied. 	RAA does not require Rrs to take any specific action on DN that are subject to abuse reports. Any action that a Rr may take against a reported DN will depend on the Rr's own policies and review of the details of each case

Response by Contractual Compliance (4c)

- ⦿ **Q4c. Challenges in determining compliance failure by a CP**
 - **No challenges in determining whether a CP fails to comply**
 - During investigation, CC relies on complaint received + supporting evidence, reference to relevant contractual provision and itemized list of information and record to demonstrate compliance
 - RAA does not prescribe specific consequences that Rrs must impose on DN that are subject to abuse report – so, CC has not contractual authority to demand imposition or specific action by Rrs
 - RA Spec. 11, s. 3(a) only requires RO to compel Rr-registrant agreement to prohibit registrants from engaging in certain activities with threat of DN suspension – does not provide ICANN org with authority to instruct Rr to impose consequences.
 - In summary, CC does not face any challenges in enforcing the RAA and RA obligations as they are written. If and when new obligations are imposed either through community policy development or new contractual terms, CC will enforce those as well so long as they are unambiguous and enforceable.

Response by Contractual Compliance (5)

- ⦿ **Q5. Challenges in remediating non-compliance by a CP**
 - CC derives its authority from agreements between ICANN Org and CPs (i.e. RA, RAA)
 - Enforcement includes ability to (a) suspend or terminate RAA; or (b) terminate RA
 - **No challenges in utilizing tools provided by contracts** – the tools and length of processes against non-compliance vary depending on Rr vs RO.

 - If Rr fails compliance with abuse-related requirements specifically included in RAA during informal resolution stage, CC issues formal notice of breach
 - – if this notice isn't cured, ICANN may escalate to suspension (for up to 12 months) of Rr's ability to register new DNs or accept inbound transfers or to terminate RAA

 - If RO fails compliance with abuse-related requirements specifically included in RA during informal resolution stage, CC issues formal notice of breach
 - - if this notice isn't cured, ICANN may initiate termination proceedings per RA, including mediation and arbitration phases.