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

Part 2 presentation to CPWG on 25 May 2022

Justine Chew
Member, GNSO Council Small Team on DNS Abuse

23 May 2022

ICANN
AT-LARGE

Context

- 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 in mid Apr 2022 onwards
- **Still at preliminary observation stage; final output pending**

Outreach on DNS Abuse

- **ACs, SG/Cs, DNSAI**

  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*

- **Contractual Compliance**

  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*

PART 1: Preliminary Observations by GC Small Team of Responses from ACs, SG/Cs & DNSAI

TO BE DISCUSSED AT A LATER DATE

PART 2: Responses from ICANN Contractual Compliance which are being reviewed by GC Small Team

Response by Contractual Compliance (1)

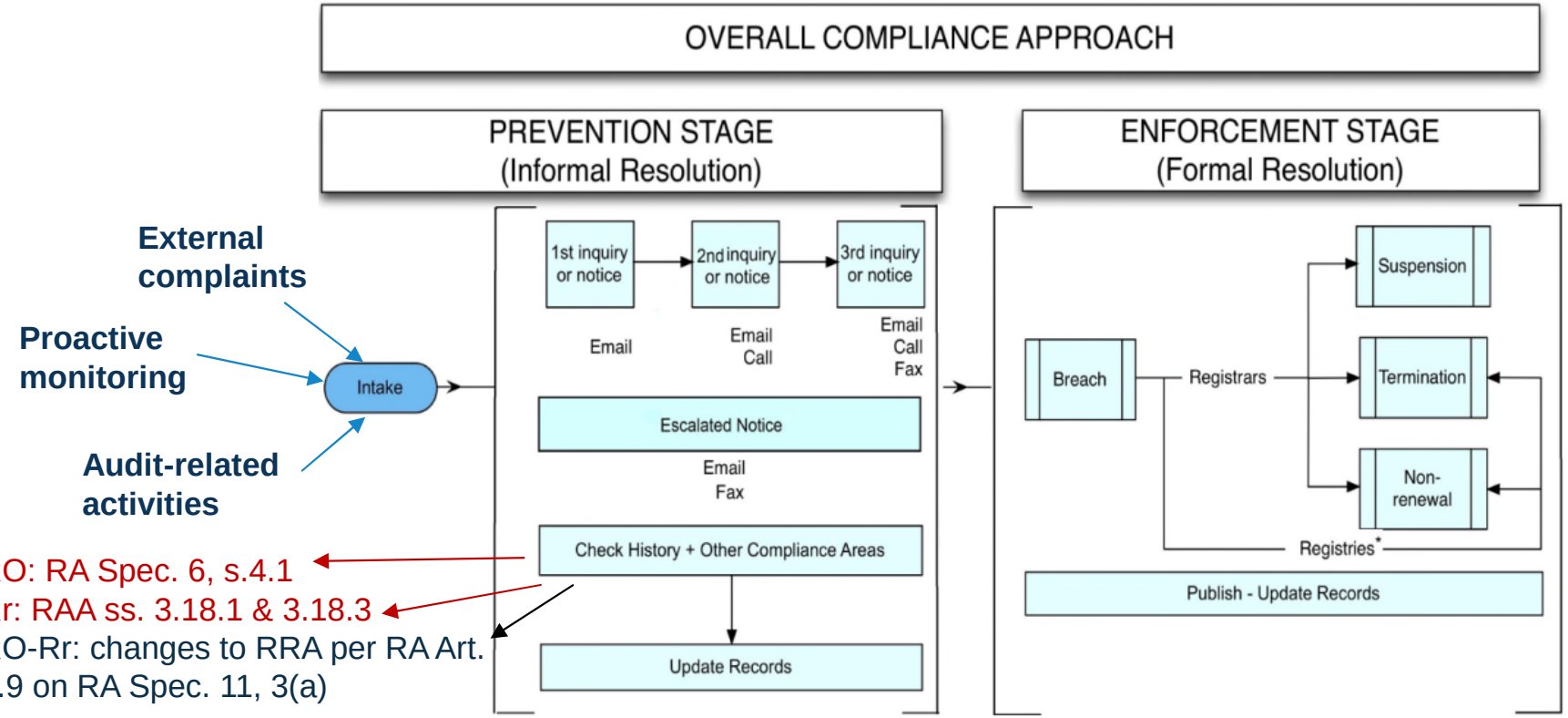
Q1. CC enforces vide RA, RAA and others

Registry Agmt (RA)	Registrar Acc Agmt (RAA)
Spec. 6, s. 4.1 – RO to publish accurate details - valid email, mailing address, primary contact for queries on malicious conduct in TLD	**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
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	**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.
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?*	

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



- RO: RA Spec. 6, s.4.1
- Rr: RAA ss. 3.18.1 & 3.18.3
- RO-Rr: changes to RRA per RA Art. 2.9 on RA Spec. 11, 3(a)

- 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	• 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	• 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	• 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	• 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.