Responses to SSR2 Questions of 26 April 2019

1. Tell us about Compliance's access to, and use of, WHOIS.

ICANN Contractual Compliance monitors registrar compliance with WHOIS requirements and, in addition to addressing third party complaints, proactively addresses systemic and trending areas of noncompliance through, for example, outreach activities.

WHOIS data is also accessed to validate several complaint types, e.g. complaints related to transfer or domain name renewals. Where the data is not publicly accessible, Compliance requests the specific unredacted registration data that is needed for the review and validation of the complaint at hand from the contracted party.

Details can be found in published reports at https://www.icann.org/resources/pages/compliance-reports-2018. Registrars that are unable to demonstrate compliance are "sanctioned" via enforcement actions and de-accreditation.

ICANN org also mitigates noncompliance through its published materials on icann.org and frequent outreach and engagement efforts regarding contractual obligations.
See https://www.icann.org/resources/compliance/outreach as an example.

Examples of Compliance tools used include the compliance ticketing system (to receive complaints), the compliance email address compliance@icann.org, an internal system used for monitoring WHOIS service availability, an internal system used for registrar and registry data (RADAR, Naming Service portal, Registrar Info status tool (to check domains under registration reported monthly), ICANN WHOIS and manual checks of port 43 WHOIS and contracted parties' web-based WHOIS service.

2. Tell us about Compliance's approach with contracted parties that have systemic 'overwhelming rates of abuse.

Contractual Compliance monitors compliance with Section 3.18 of the 2013 RAA through processing abuse complaints submitted through the Registrar Standards Complaint Form (https://forms.icann.org/en/resources/compliance/complaints/registrars/standards-complaint-form) and by conducting the Registrar Audit Program which includes the obligations of Sections 3.18.1, 3.18.2 and 3.18.3 of the 2013 RAA.
For abuse complaints, ICANN collects evidence from the reporter and confirms that the reporter sent abuse report(s) to the registrar's abuse contact email address before sending the complaint to registrar.
Once confirmed, ICANN could request the registrar to provide:

1. A description of the steps taken to investigate and respond to abuse report
2. The amount of time taken to respond to abuse report
3. All correspondence with complainant and registrant
4. The link to website's abuse contact email and handling procedure
5. The location of dedicated abuse email and telephone for law-enforcement reports
6. The registrar's WHOIS abuse contacts, email address and phone number
7. Examples of steps registrars have taken to investigate and respond to abuse reports include:

Contacting the registrant
Requesting and obtaining evidence or licenses
Providing hosting provider information to complainant
Performing Whois verification
Performing transfer upon request of registrant
Suspending domain

Several blogs have been published on this topic; please refer to the ICANN Contractual Compliance Reports & Blogs page dating back to 2015. For more details on the abuse handling and resolution, please refer to slides 19 - 24 in the Registrar Compliance Program material.

In addition, ICANN launched a DNS infrastructure abuse-focused audit for about 1200 gTLDs in November 2018, and held two audit webinars (recordings for 1st webinar and 2nd webinar) with the registries to address their questions and concerns. Some of these concerns were also raised in a recent email from the Registry Stakeholder Group and addressed by Contractual Compliance. For the first time, and to help prepare for the upcoming audit, Contractual Compliance sent the auditees the complete list of gTLDs that are included in the audit, and a pro-forma list of questions and data requests that will be included in the November 2018 Registry Audit round. For more information about the audit, please read this blog.

3. Tell us about the volume over the last few years of enforcement actions and how Compliance has selected auditing and enforcement targets.

Monthly dashboards containing complaint volume information can be found here: https://features.icann.org/compliance/dashboard/report-list
Notices of Breach, Suspension, Termination and Non-Renewal can be found here: https://www.icann.org/compliance/notices
Historical reports and blogs can be found here: https://www.icann.org/resources/pages/compliance-reports-2018

ICANN uses the following factors in its process to select parties for audit:
Contracted parties that have not been previously audited
Contracted parties that were audited over 2 years ago
Contracted parties with highest numbers of 3rd Notices per number of domains under management calculated over the past 12 months
Contracted parties that had received a Notice of Breach in last 12 months
Contracted parties with highest numbers of failed data escrow deposits
Contracted parties with low responsiveness to ICANN's requests/inquiries
Contracted parties with issues that were remediated and are re-occurring again
Contracted parties for which there appear to be ICANN community concerns, as reflected in media reports, blogs, or inquiries/reports from community members or other contracted parties
Contracted parties that had changes to the delivery of services (for ex. Changes in service providers, data escrow agents, etc.)
Please see https://www.icann.org/resources/pages/faqs-2012-10-31-en#Audit_Methodology_Questions for FAQ’s on the audit process.

In addition, DAAR data is used to assist the ICANN organization's Contractual Compliance department in obtaining additional information relating to Domain Name System (DNS) abuse for an accredited registrar or TLD registry operator. Please refer to the ICANN Contractual Compliance Audit Program FAQs at https://www.icann.org/resources/pages/faqs-2012-10-31-en for more information regarding its use.

Awareness of the prevalence of DNS infrastructure abuse has grown significantly as a result of DAAR, the CCT Review Team report, and other publicly available information.

The current Registry Operator(RO) audit focuses on reviews of:

- ROs' security threats reports for completeness in comparison to publicly available reports and ICANN DAAR, and
- Processes, procedures and handling of DNS infrastructure abuse by RO's
- New gTLDs have specific Public Interest Commitments in their respective Registry Agreement under Specification 11.
- Some Legacy gTLDs do not have such obligations. The objective here is to learn about their procedures in handling DNS abuse and security threats, if any.

4. Describe how issues are flagged, how Compliance proceeds with contracted parties and complainants, and what your main obstacles and challenges are when dealing with violations.

Issues are flagged as a result of complaints, proactive monitoring and others are audit-related.

The complaints are received by ICANN upon submission by complainants using the web forms posted at this link: https://www.icann.org/compliance/complaint or via an email to Compliance@ICANN.org.

The monitoring activities are ICANN-initiated, based in part on industry articles, social media postings, previous complaints, and trend analysis in an effort to proactively address any alleged failure to comply with contract terms.

Please refer to this link https://www.icann.org/resources/pages/audits-2012-02-25-en to learn more about ICANN Contractual Compliance Audit program and activities.

Contractual Compliance follows the ICANN Approach and Process described here when processing complaints. The informal resolution process or Prevention stage is between ICANN and the contracted parties and is kept confidential to allow collaboration. However, if a Contracted Party fails to respond or demonstrate compliance during the Prevention stage, ICANN may transition to the Enforcement Stage by issuing a public enforcement notice, such as a Notice of Breach. Failure to cure a noncompliance following the issuance of a Notice of Breach may results in suspension (Registrars only) or termination of the Contracted Party's agreement. ICANN may also initiate legal action against the Contracted Party and require payment of ICANN's costs and expenses, including attorney fees, associated with enforcing the contract, among other actions. All enforcement notices issued by ICANN Contractual Compliance are posted here and a list of enforcement notice reasons for the prior 13 rolling months can be found here.

Challenges and delays in enforcing have been caused, in some instances, by reporters not timely and fully responding to requests for information and evidence to validate complaints, as well as lack of specificity of the language pertaining to certain contractual obligations.

5. What parts of the contracted party agreements that Compliance audits and enforces do you think are effective in supporting DNS security, stability and resiliency?

ICANN Contractual Compliance uses the ICANN Contractual Compliance Approach and Process to process third party complaints and conduct proactive monitoring and audits related to registrar and registry operator security, stability and resiliency issues, including those related to DNS abuse, WHOIS accuracy, WHOIS service and format issues, data escrow, other critical registry technical functions and reserved names and names collision occurrence management. Information and metrics regarding these activities can be found on the ICANN Contractual Compliance pages of icann.org.

6. What part of these contracts do you think hinder Compliance in any way from effectively addressing the levels of abuse involving contracted parties?

Through the ongoing audit of registries' compliance with their DNS abuse obligations, we have observed a lack of certainty surrounding the scope of those obligations. In addition, the lack of an explicit contractual prohibition on systematic DNS abuse makes it difficult for ICANN compliance to address it. A consensus policy that defines and prohibits DNS abuse, and is incorporated into the agreements with the contracted parties, would allow ICANN Compliance to play an effective enforcement role in support of the community's policies.