ICANN 66

ANNUAL GENERAL

MONTRÉAL

2–7 November 2019

Agenda - Contractual Compliance & GDD

- Registry Audit and Specification 11 3(b) Interpretations
- Centralized Zone Data Service (CZDS) Access Issues
- Upcoming Changes to Technical Validations & Monitoring
- GDD Structure
- 2020 GDD Industry Summit
- Information Transparency Initiative (ITI) Update
- RDAP - RA/RAA Amendments
- Policy Implementation Updates
- Operational Improvements to PICDRP Update
- Appendix
  - Additional CZDS information and FAQ
  - Extending ERSR waivers to Registrars

Registry Audit and Specification 11 3(b) Interpretations

Introduction

- There are a number of discussions within the ICANN community regarding DNS security threats

- This discussion with the Registry Stakeholder group is limited to how to interpret an existing contractual provision:

  RAA Spec. 11 3(b) "*Registry Operator will periodically conduct a technical analysis to assess whether domains in the TLD are being used to perpetrate security threats, such as pharming, phishing, malware, and botnets. Registry Operator will maintain statistical reports on the number of security threats identified and the actions taken as a result of the periodic security checks. Registry Operator will maintain these reports for the term of the Agreement unless a shorter period is required by law or approved by ICANN, and will provide them to ICANN upon request.*"

Areas of agreement

1. Registry Operators must periodically conduct a technical analysis (scan of their TLD zone) to identify domains used to perpetrate security threats

2. For the purposes of this provision and the recent audit, security threats are phishing, malware and botnets.

3. Registry Operators must maintain statistical reports on the number of security threats identified and the actions taken as a result of the periodic security checks.

4. Registry Operators must maintain the reports and provide them to ICANN upon request in the form of Security Threat Reports (STRs).

Areas of disagreement

- Some ROs submitted STRs that included information about specific domains involved in abuse (rather than aggregated statistical data only)
  - Compliance compared the domains listed to security threats identified by publicly available RBLs in the same timeframe.
  - Any variances were presented to ROs as observations with a request to review the variances (reviewing a sample of domains was acceptable) to assess whether there were gaps in the ROs' monitoring systems and/or inaccuracies in the publicly available data.

- Some ROs do not interpret the Specification to obligate them to share the details of their existing DNS security threat programs with Compliance or information about specific domains investigated (as opposed to aggregated statistical information).
  - In these cases, it was not possible to determine the cause of any discrepancies between STR data and the number of security threats reported by RBLs, making it difficult to form a judgment as to whether their efforts to mitigate DNS security threats are effective.

Areas of disagreement (continued)

- The primary disagreements among ICANN Compliance and some ROs are:
  1. Whether ROs must provide detailed information with ICANN Compliance regarding their DNS security threat programs, including the list of domains identified by the RO as security threats, and
  2. Whether it is appropriate for ICANN Compliance to identify and provide to ROs the variance in reported DNS security threats included in ROs' STRs versus those listed in RBLs.

- To address this issue, ICANN org proposes to enter into a dialogue with Registry Operators to develop a shared understanding of the scope of Specification 11 3(b).

- Next steps?

Centralized Zone Data Service (CZDS) Access Issues

Common issues + Requests to RySG

From January 2017 to September 2019, ICANN Compliance processed over 2,000 complaints regarding CZDS access.

- Of the 2,000+ complaints, 1,200 were approved by the Registry Operator after ICANN Compliance sent inquiries. It is possible that Registry Operators may not have processes in place to regularly review zone file access requests/renewals, or they are unaware of auto-approval functionality.
- The 2,000 complaints are tied to about 450 TLDs in total. Approximately half are “Brand” TLDs. Compliance’s experience in processing suggests this group of Registry Operators may require additional education on CZDS and Zone Files.
- Some Registry Operators are preemptively denying requests with the expectation that the user provide evidence to demonstrate they would be acting in accordance to the listed conditions within Specification 4 Section 2.1.5. Complaints filed are mostly by industry researchers and some RO’s are not clear what information is in the Zone Files.
- Some Registry Operators will request access to NSP after receiving inquiries from Compliance. Based on Compliance experience, zone file access request processing may not be fully handed over when turnover occurs.

Common issues + Requests to RySG

Asks of the Registry Stakeholder Group:

Please help us educate the Registry Operators on CZDS obligations as follows:

- Share your CZDS experience with other Registry Operators, especially those that do not attend ICANN meetings and the “Brand”(Spec 13) TLDs.
- Share details regarding what data is in the zone files when granting CZDS access.
- Share your CZDS request review process with other Registry Operators.
  - How often the reviews and approvals take place?
  - What information do you look for when reviewing?
  - What makes you comfortable with approving the request?
  - What do you do if there is a request that you have questions on?
  - If you use the auto-approval function, what makes you comfortable doing that?
- Share your handover process in relation to CZDS approvals when people leave your company.

Upcoming Changes to Technical Validations & Monitoring

Additional Validations in BRDA

- Does not include additional data included in the deposit, e.g.:
  - Contact, IDN, NNDN, EPP Param objects
  - Registrant or contact attributes in domain object

- File format complies with:
  - Registry Data Escrow Specification
  - Domain Name Registration Data Objects Mapping

- Mandatory elements and data are present

- Correct TLD and Watermark

- Correct deposit type (i.e., “FULL”)

- Correct CRC32 checksum (for CSV files)

- File names are of the form:
  - {gTLD}_{YYYY-MM-DD}_thin_S{#}_R{rev}.{ext}

Additional Measurements in SLA Monitoring

Service Level Requirements to be implemented:

Parameter	SLR (monthly basis)
DNS name server availability	≤ 432 min of downtime (≈ 99%)
TCP **DNS** resolution RTT	≤ 1500 ms, for at least 95% of the queries
UDP **DNS** resolution RTT	≤ 500 ms, for at least 95% of the queries
RDDS availability	≤ 864 min of downtime (≈ 98%)
RDDS query RTT	≤ 2000 ms, for at least 95% of the queries

Per section 2 of Specification 10 of the Agreement, Service Level Requirements are measured on a monthly basis

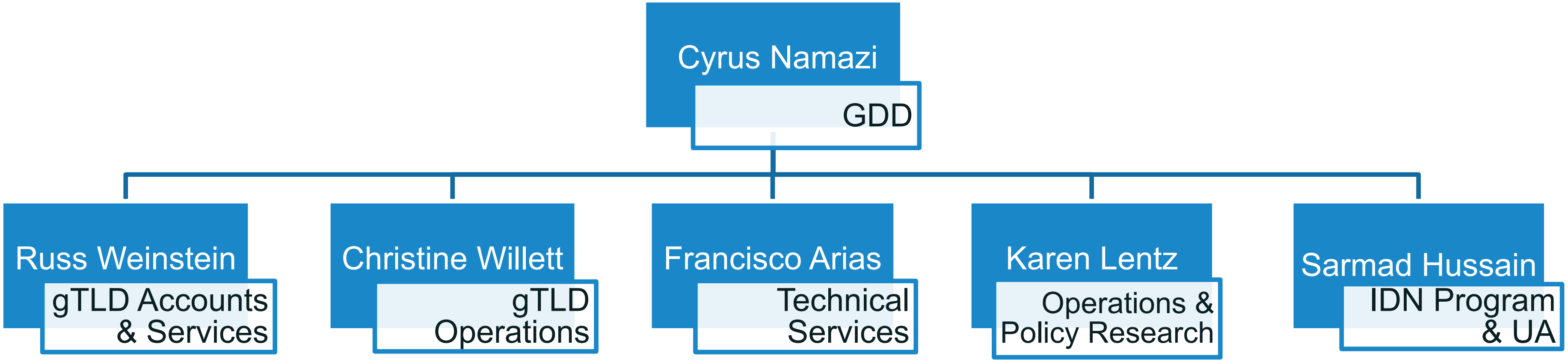
The Service Level measurements of a given month will be generated at the beginning of the following month as specified in section 3 of Specification 10 of the Agreement

Compliance Enforcement Approach

Once monitoring projects are in production, Compliance will process any referrals in the following manner:

- For manual referrals, Compliance will review to ensure that the incoming data is reliable and within the scope of the relevant ICANN agreement and consensus policies.
- If needed, Compliance follows up with the Technical Services or other departments within the ICANN organization for additional information.
- Compliance works with registries to resolve contractual compliance matters via 1-2-3 inquiry/notice or an escalated notice.
- Compliance reviews responses from contracted parties and, as needed, consults with other departments in the ICANN organization.
- Once resolved, Compliance informs the contracted party via a closure notice.
- ICANN's Contractual Compliance Approach and Processes may be found here: https://www.icann.org/resources/pages/approach-processes-2012-02-25-en

ICANN org Global Domains Division (GDD) Structure



Cyrus Namazi
GDD

Russ Weinstein
gTLD Accounts & Services

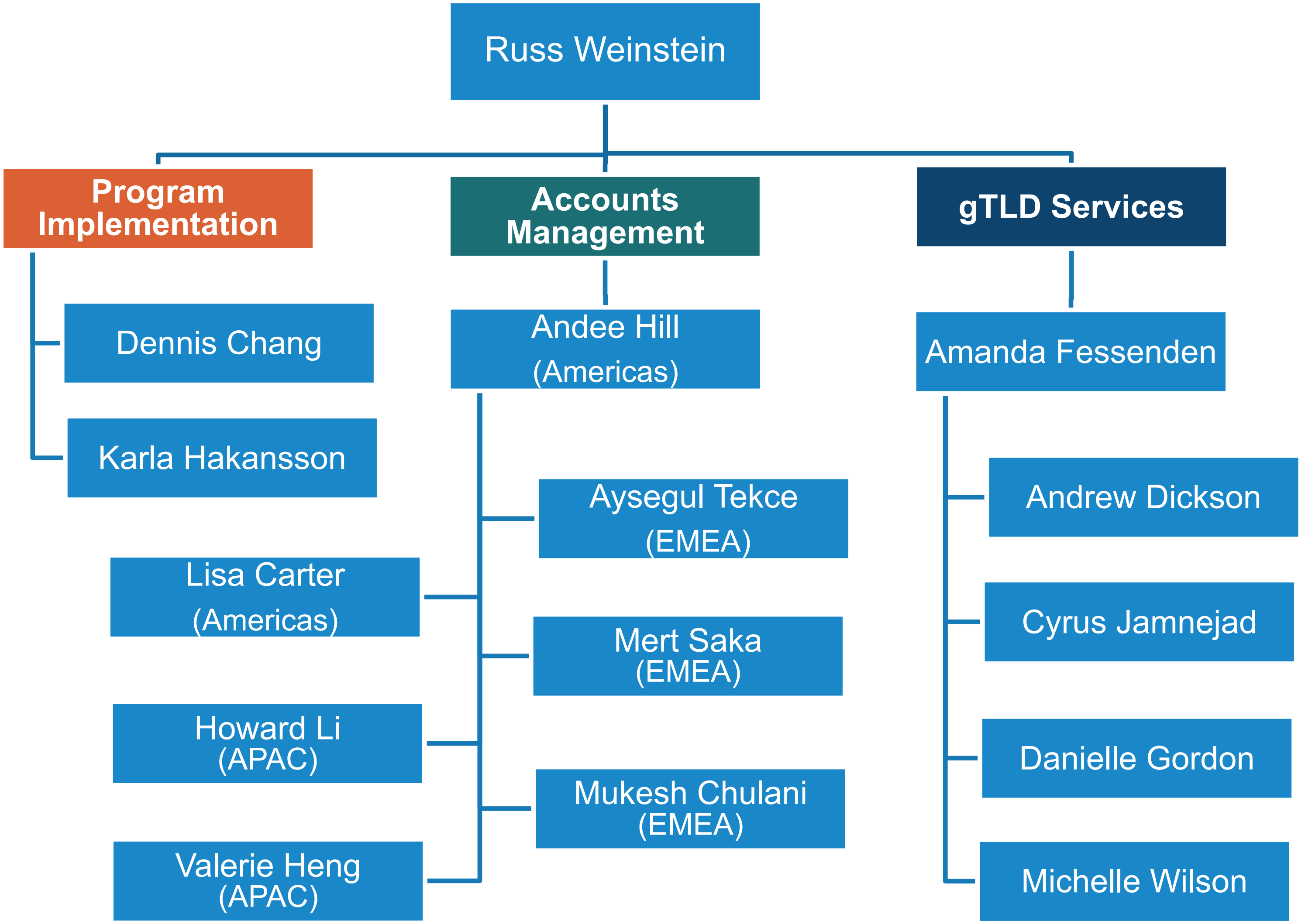
Christine Willett
gTLD Operations

Francisco Arias
Technical Services

Karen Lentz
Operations & Policy Research

Sarmad Hussain
IDN Program & UA

gTLD Accounts & Services Team Structure



Russ Weinstein

Program Implementation

- Dennis Chang
- Karla Hakansson

Accounts Management

- Andee Hill (Americas)
  - Aysegul Tekce (EMEA)
  - Lisa Carter (Americas)
  - Mert Saka (EMEA)
  - Howard Li (APAC)
  - Mukesh Chulani (EMEA)
  - Valerie Heng (APAC)

gTLD Services

- Amanda Fessenden
  - Andrew Dickson
  - Cyrus Jamnejad
  - Danielle Gordon
  - Michelle Wilson

2020 GDD Industry Summit

Other Events	Dates (May 2020)
Registration Operations Workshop (ROW)	6
DNS Symposium	7 – 8
DNS Operations, Analysis, and Research Center (OARC)	9 – 10

- Venue: Paris Marriott Rive Gauche Hotel & Conference Center
- Interested in crafting the **GDD Summit agenda**?
  Email globalsupport@icann.org to join the Planning Committee
- Check out **sponsorship** opportunities at https://www.icann.org/gddsummit
- **2021 GDD Industry Summit**:
  Looking for venues in the Los Angeles, California area

ITI Update on Progress

The Information Transparency Initiative (ITI) is an operational activity to improve ICANN.org's content governance and infrastructure:

Enhancing search through a new information architecture and first-ever consistent taxonomy.

Improving user experience for features like Public Comment and Content Subscriptions.

We need your input!

Read the latest ITI blog on ICANN.org for details on current content available for feedback.

Visit feedback.icann.org and share your comments.

ITI Timeline: November 2019 - September 2020

Nov 2019

Registry Agreements Available On Feedback Site

Nov 2019

Conducting Community Focus Groups on the new Navigation

Nov 2019

Board Meeting Materials Available on Feedback Site

Jan 2020

Public Comment Available on Feedback Site

April 2020

Soft Launch of New ICANN.org

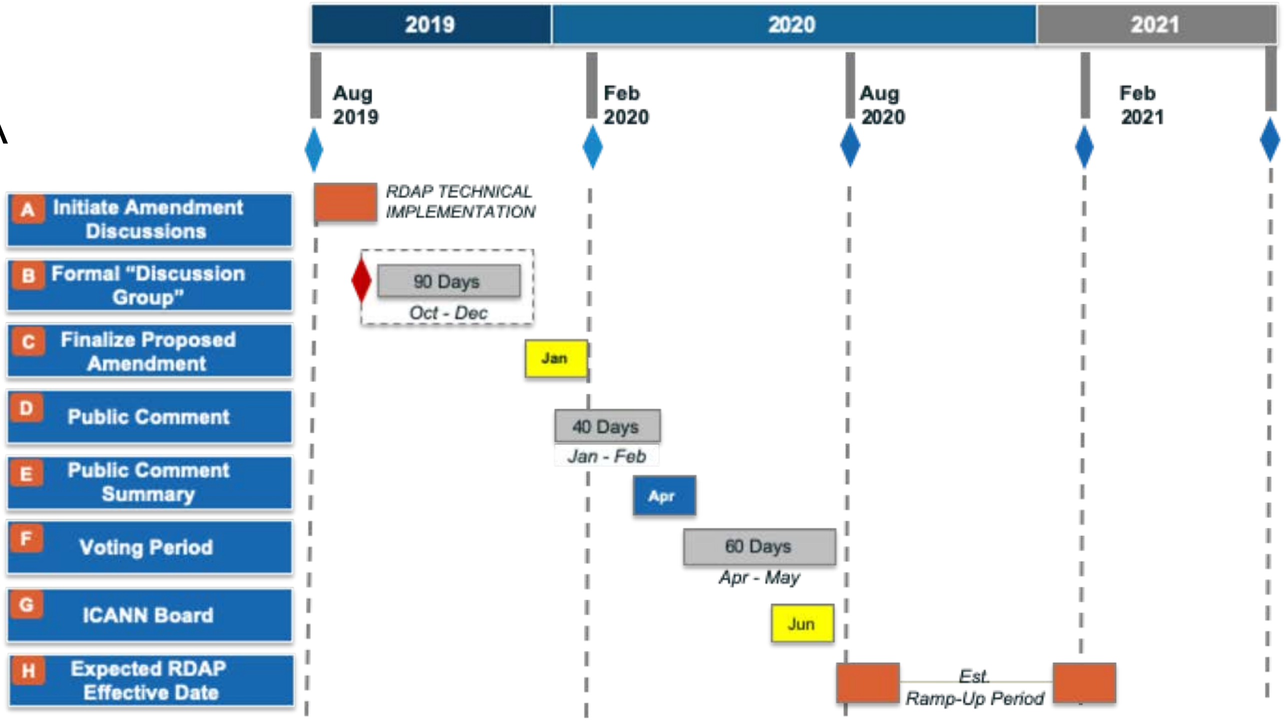
Sept 2020

Launch of New ICANN.org

RDAP - RA/RAA Amendments

- 21 October: ICANN org triggered the contracts amendment process with the RySG and RrSG.

- Focus is to amend the RA and RAA to:
    - incorporate contractual requirements comparable to the WHOIS services for RDAP
    - define a coordinated transition from WHOIS to RDAP

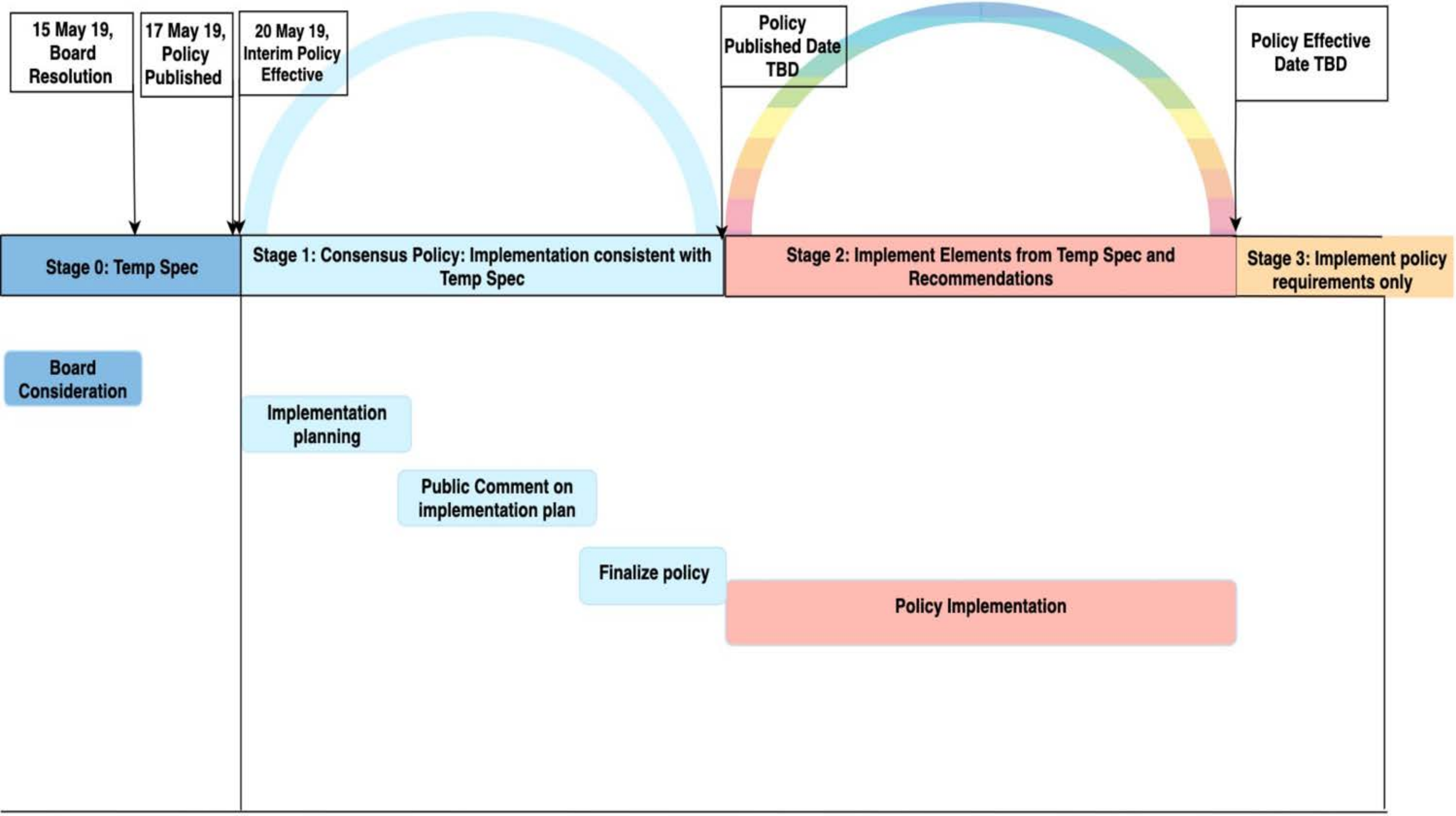


- Plan includes efforts to raise global awareness of what's changing with the introduction of RDAP

Registration Data Policy Implementation

1. The Board adopted the EPDP Phase 1 Final report on 15 May 2019 (two exceptions)
2. Implementation team working with *Pre-IRT* published the Interim Registration Data Policy on 17 May 2019
3. IRT convened 29 May 2019: 35 members, 36 observers
4. Currently engaged in analysis of the recommendations to determine the work plans, implementation requirements, policy languages, and estimate the implementation tasks.
   - **a. Rec 27** work plan shared with GNSO Council
   - **b. Rec 15** reports were provided to EPDP Phase 2 Team
5. Project timeline will be determined upon completion of the analysis and design of the implementation approach
6. Two IRT meetings scheduled at ICANN66
   - a. 8:30 - 10:15 Wednesday, 11 Nov 2019
   - b. 8:30 - 10:15 Thursday, 12 Nov 2019

Stages of the Reg Data Policy



15 May 19, Board Resolution
17 May 19, Policy Published
20 May 19, Interim Policy Effective
Policy Published Date TBD
Policy Effective Date TBD
Stage 0: Temp Spec
Stage 1: Consensus Policy: Implementation consistent with Temp Spec
Stage 2: Implement Elements from Temp Spec and Recommendations
Stage 3: Implement policy requirements only
Board Consideration
Implementation planning
Public Comment on implementation plan
Finalize policy
Policy Implementation

Protection for Certain Red Cross Names in All gTLDs

- This is a policy amendment to the published policy for the Protection of the IGO & INGO Identifier for All gTLDs.
- The Reconvene PDP WG developed a list of specific names of 191 Red Cross Names as well as a limited, defined set of variants for these names to be added to the reserved names list.
- On 27 Jan 2019, the ICANN Board adopted the recommendation.
- On 23 Oct 2019, the Implementation Team opened public comment for the implementation plan that includes over 7000 DNS Labels
- The public comment closes on 12 Dec 2019
- Target date for the policy publication is 1 Feb 2020 with 1 Aug 2020 effective date

Operational Improvements to PICDRP Update

- Public Interest Commitments Dispute Resolution Procedure (PICDRP) was established in December 2013
- Based on ICANN org Compliance's experience and Complaints Office recommendations for **operational improvements** to:
  - Provide clear guidelines about what type of information should be shared with the involved parties, and when in the PICDRP
  - Disclose identities of selected panelists to the parties
  - Set timing expectation as to when the panel will be appointed
  - Publish all panel reports
- The Registry Agreements utilizing the PICDRP allow ICANN org to make limited revisions of the procedure
- Collaborated with the RySG to review the changes to the PICDRP
- Finalizing the changes in November 2019

Appendix

Additional CZDS information and FAQ

RA Specification

- Specification 4, Section 2 of the registry agreement (RA) requires Registry Operators to provide access to gTLD zone files through the Centralized Zone Data Service (CZDS).

- Reasons for denying access under Specification 4:
  - Incorrect or illegitimate credentialing requirements of Section 2.1.2
  - Reasonable belief requestor will violate terms of Section 2.1.5

- Reasons for revoking access under Specification 4:
  - Registry Operator has evidence to support that the user has violated the terms of Section 2.1.5

- ICANN is working on a FAQ for Registry Operators regarding CZDS, but is requesting the RySG to assist with educating fellow community members on the nature of zone files and zone file access.

Explanation of Zone Files & Zone File Access

- **What are zone data and zone files?**

The Registry Operator's zone data contains the mapping of domain names, associated name server names, and IP addresses for those name servers. These details are updated by the Registry Operator for its respective TLDs whenever information changes or a domain name is added or removed.

Each Registry Operator keeps its zone data in a text file called the Zone File which is updated once every 24 hours.

- **Who needs access to the zone data?**

Zone file access provides anticrime organizations, businesses, cybersecurity professionals, law enforcement, and researchers with a means to download the entire zone file "in bulk." These organizations apply the bulk zone data to combat phishing, spam, brand and trademark infringements, and other malicious uses of domains.

Explanation of Zone Files & Zone File Access

- **Why should a Registry Operator provide users with CZDS access?**

Registry Operators have a contractual obligation to provide access under Section 2, Specification 4 of the Registry Agreement. The CZDS was established by the community as part of the development of the new gTLD program to help protect Internet users.

- **What are the security measures in place for giving access to these users?**

Users are required to provide cryptographic keys when they create their account at czds.icann.org for secure zone file transmission.

Explanation of Zone Files & Zone File Access

- **What are the compliance measures being taken by ICANN for users who have been granted access and ensuring that it is not being misused?**

ICANN does not enter into contracts with the users of the zone file data. However, Section 2.1.1(b, c), Specification 4 provides that a Registry Operator can deny or revoke access if it has evidence to support that the user will violate or has violated the terms of Section 2.1.5.

- **What is the consequence of denial of access?**

If the Registry Operator denies a request for access to the zone file of a TLD that it operates, and the reason for such denial is not within the valid reasons for denial per the Registry Agreement and its specifications, the Registry Operator may be in breach of its contract with ICANN.

Metrics

- From January 2017 to September 2019, ICANN Compliance processed over 2000 complaints regarding CZDS access requests.

- About 500 complaints were filed in 2017 and 2018 respectively, with over 1000 complaints filed between January 2019 and September 2019. The complaints relate to over 450 TLDs.

- Of the 2000+ complaints, 1,200 were approved by the Registry Operator after Compliance sent the Registry Operator inquiries.

- Approximately 500 complaints were approved by the time Compliance began its review of the complaints, and were closed without sending inquiries to the Registry Operator.

- Of the 2000+ complaints, approximately 150 concerned denial/revocation of access.

- Approximately 200 complaints were duplicate complaints, where the reporter had filed multiple complaints regarding the same TLD, and were closed without sending inquiries to the registry operator.

Common Issues

- Registry Operators denying zone file access requests due to security concerns regarding Zone Files, which may be due to a lack of understanding regarding zone file content. In such cases, Registry Operators are preemptively denying requests with the expectation that the user provide evidence to demonstrate they would be acting in accordance to the listed conditions within Specification 4 Section 2.1.5.

- From January 2017 to September 2019, ICANN Compliance processed over 2000 complaints regarding CZDS access. Of the 2000+ complaints, 1,200 were approved by the Registry Operator after Compliance sent inquiries. Approximately 500 complaints were approved by the time Compliance reviewed the complaints, and approximately 200 complaints were duplicate complaints, where the reporter had filed multiple complaints regarding the same TLD. Based on this data, there is a high probability that many Registry Operators may not have formalized processes in place to regularly review zone file access requests/renewals, or their internal SLAs extend beyond certain community expectations, or they are unaware of auto-approval functionality.

Common Issues

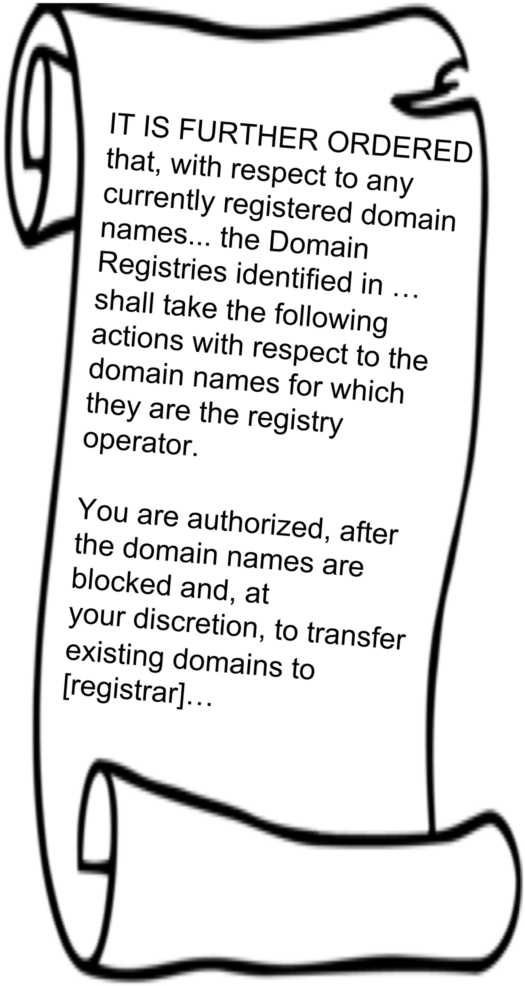
- After being contacted by Compliance regarding pending request for zone file access, some Registry Operators require assistance from ICANN in establishing credentialed contacts to process such requests. This indicates that responsibilities regarding zone file access request processing are not often communicated internally when turnover occurs.

Extending ERSR waivers to Registrars

Expedited Registry Security Request (ERSR): Scope

- **Service for gTLD Registry Operator (RO) to inform ICANN of a present or imminent security incident to their TLD and/or the DNS and to request contractual waiver for actions to mitigate or eliminate an incident.**
  - The ERSR is exclusively for Incidents, i.e., requiring immediate action by the RO and an expedited response within 3 business days from ICANN.
  - An Incident could be one or more of the following:
    - Malicious activity involving the DNS of scale and severity that threatens systematic security, stability and resiliency of a TLD or the DNS;
    - Unauthorized disclosure, alteration, insertion or destruction of registry data;
    - Unauthorized access to or disclosure of information or resources on the Internet by systems operating in accordance with all applicable standards;
    - An occurrence with the potential to cause a temporary or long-term failure of one or more of the critical functions of a gTLD registry
  - Contractual waiver is an exemption from compliance regarding specific provision(s) of the Registry Agreement (RA) for the time period necessary to respond to the incident.

Opportunity to Further Improve Current ERSR Process



IT IS FURTHER ORDERED that, with respect to any currently registered domain names... the Domain Registries identified in … shall take the following actions with respect to the domain names for which they are the registry operator.

You are authorized, after the domain names are blocked and, at your discretion, to transfer existing domains to [registrar]…

- **Example: In response to a court order to address present or imminent security incidents, ROs may transfer impacted domain names to ICANN-accredited Registrars (Rrs). However, while the ERSR's waiver provisions apply to ROs, they do not currently extend to any cooperating Rrs.**
- Conceptually, among the most common base gTLD provisions requested to be waived by ROs as part of an ERSR waiver request would appear to also apply to cooperating Rrs:
  - Section 6.1(a)(ii) and 6.3: Registry-Level Fees
  - Section 2.4 of Specification 3: Registry Operator Monthly Reporting

ICANN org is currently reviewing further improvements that can be made to the ERSR process.

We are interested to hear your input on this and other potential ERSR-related gaps.

Engage with ICANN – Thank You and Questions

ICANN

One World, One Internet

Visit us at **icann.org**

- @icann
- facebook.com/icannorg
- youtube.com/icannnews
- flickr.com/icann
- linkedin/company/icann
- slideshare/icannpresentations
- soundcloud/icann