ICANN BOARD OF DIRECTORS
SUBMISSION NO. 2020-12-11-1b

TITLE: **Appointment of Root Server System Advisory Committee (RSSAC) Chair**

PROPOSED ACTION: **For Board Consideration and Approval**

EXECUTIVE SUMMARY:

Per Article 12, Section 2, Subsection C (ii) of the ICANN Bylaws, the Root Server System Advisory Committee (RSSAC) submits the following member for appointment as the chair of the RSSAC:

- Fred Baker, Internet Systems Consortium

Fred Baker has been re-elected by acclamation to serve as the RSSAC chair for a two-year term beginning 1 January 2021.

RSSAC RECOMMENDATION:

The RSSAC recommends the ICANN Board of Directors appoint Fred Baker as the RSSAC chair for a two-year term beginning 1 January 2021.

PROPOSED RESOLUTION:

Whereas, the ICANN Bylaws call for the establishment of the Root Server System Advisory Committee (RSSAC) with the role to advise the ICANN community and ICANN Board of Directors on matters relating to the operation, administration, security, and integrity of the Internet's Root Server System.

Whereas, the ICANN Bylaws call for the RSSAC to be led by a chair that would be appointed by the ICANN Board of Directors.

Whereas, the RSSAC went through a 30-day nomination period for the RSSAC chair election process.

Whereas, Fred Baker was the only candidate and re-elected by acclamation on 1 December 2020.

Whereas, the RSSAC has recommended to the ICANN Board of Directors the appointment of Fred Baker as the RSSAC chair.

Resolved (2020.12.17.XX), the ICANN Board of Directors appoints Fred Baker as the RSSAC chair through 31 December 2022.

PROPOSED RATIONALE:

In September 2019, the ICANN Board of Directors approved the Standard Bylaws amendment process pertaining to the RSSAC leadership. As a result, the RSSAC leadership composition transitioned from two co-chairs to a chair and a vice chair. The current term for the RSSAC chair Fred Baker expires 31 December 2020.

The appointment of the RSSAC chair is not anticipated to have any fiscal impact on the ICANN organization that has not already been accounted for in the budgeted resources necessary for ongoing support of the RSSAC.

This resolution is an organizational administrative function for which no public comment is required. The appointment of the RSSAC chair contributes to the commitment of the ICANN organization to strengthen the security, stability, and resiliency of the DNS in the public interest and in accordance with ICANN's mission.

Submitted by:	Kaveh Ranjbar
Position:	RSSAC Liaison to the ICANN Board
Date Noted:	2 December 2020
Email and Phone Number	kaveh.ranjbar@board.icann.org

ICANN BOARD PAPER NO. 2020.12.17.1c

TITLE: **Security and Stability Advisory Committee (SSAC) Member Appointments**

PROPOSED ACTION: **For Board Consideration and Approval**

EXECUTIVE SUMMARY:

The Security and Stability Advisory Committee (SSAC) recommends the Board reappoint the SSAC members as identified in the proposed resolution, and respectfully requests the appointment of Matthew Thomas as a new Committee member.

COMMITTEE RECOMMENDATION:

The Committee desires two actions from the ICANN Board: 1) the reappointment of the SSAC members as identified in the proposed resolution, and 2) the appointment of Matthew Thomas to the SSAC.

PROPOSED RESOLUTION:

Whereas, the Board, at Resolution 2010.08.05.07 approved Bylaws revisions that created three-year terms for SSAC members, required staggering of terms, and obligated the SSAC Chair to recommend the reappointment of all current SSAC members to full or partial terms to implement the Bylaws revisions.

Whereas, in November 2020 the SSAC Membership Committee initiated an annual review of two SSAC members whose terms are ending 31 December 2020 and submitted to the SSAC its recommendations for reappointments in December 2020.

Whereas, on 14 December 2020, the SSAC members approved the reappointments.

Whereas, the SSAC recommends that the Board reappoint the following SSAC members to three-year terms: Tim April and Andrei Kolesnikov.

Whereas, the SSAC Membership Committee, on behalf of the SSAC, requests that the Board should appoint Matthew Thomas to the SSAC for a term beginning immediately upon approval of the Board and ending on 31 December 2023.

Resolved (2020.12.17.xx), the Board accepts the recommendation of the SSAC and reappoints the following SSAC members to three-year terms beginning 01 January 2021 and ending 31 December 2023: Tim April and Andrei Kolesnikov.

Resolved (2020.12.17.xx), that the Board appoints Matthew Thomas to the SSAC for a term beginning immediately upon approval of the Board and ending on 31 December 2023.

PROPOSED RATIONALE:

The SSAC is a diverse group of individuals whose expertise in specific subject matters enables the SSAC to fulfill its role and execute its mission. Since its inception, the SSAC has invited to its membership individuals with deep knowledge and experience in technical and security areas that are critical to the security and stability of the Internet's naming and address allocation systems.

The SSAC's continued operation as a competent body is dependent on the accumulation of talented subject matter experts who have consented to volunteer their time and energies to the execution of the SSAC mission.

Matthew (Matt) Thomas is a distinguished engineer in Verisign's chief security officer (CSO) applied research division. His research focuses on numerous aspects of internet security, stability and resiliency including but not limited to DDoS attacks, domain name abuse, miscreant behavior within the Domain Name System, and large-scale measurements and evolving trends in internet architectures. Prior to joining Verisign in 2008, Matt worked for 3 years as a software engineer at AT&T. He was responsible for designing and implementing a distributed data collection system that measured and analyzed the operational performance of systems and services hosted by AT&T throughout the world. Matt is currently serving as one of the Co-Chairs of the NCAP Project.

This resolution is an organizational administrative function for which no public comment is required. The appointment of SSAC members is in the public interest and in furtherance of ICANN's mission as it contributes to the commitment of the ICANN to strengthen the security, stability, and resiliency of the DNS.

Signature Block:

Submitted by:	Merike Kaeo
Position:	Liaison to the ICANN Board from the Security and Stability Advisory Committee
Date Noted:	14 December 2020
Email:	merike.kaeo@board.icann.org

ICANN BOARD PAPER NO. 2020.12.17.1d

TITLE: **Contingency Plans for 2021 Key Signing Key Ceremonies**

PROPOSED ACTION: **For Board Consideration and Approval**

EXECUTIVE SUMMARY:

- ICANN, through PTI, must regularly generate cryptographic signatures that allow the root zone to be properly authenticated using DNSSEC. This work is typically performed every three months using "key signing ceremonies" involving trusted community representatives from throughout the world.

- In response to the Coronavirus pandemic, ICANN adopted modified procedures in April 2020 to allow essential key ceremony activity to continue with limited personnel.

- In light of the current status, ICANN Org recommends continuing to use the modified procedures for the year of 2021. In particular, these procedures would provide for a key ceremony would be held around February 2021 following the same model of the modified ceremony held in April 2020.

- Should it be safe and practical to do so, the plan envisages a return to normal ceremony operations in the 4th quarter of 2021.

ICANN ORG RECOMMENDATION:

ICANN org recommends the Board endorse the ongoing use of these contingency plans for holding the KSK ceremony, given the enduring coronavirus pandemic.

PROPOSED RESOLUTION:

Whereas, ICANN, through its affiliate PTI, must regularly generate cryptographic signatures that allow the root zone to be properly authenticated using DNSSEC. This work is currently performed every three months using "key signing ceremonies"

involving trusted community representatives from throughout the world, governed by the DNSSEC Practice Statement.

Whereas, in April 2020, the Board resolved to authorize contingency plans to hold these ceremonies in a modified format in response to the challenges posted by the COVID-19 pandemic.

Whereas, the COVID-19 pandemic continues to challenge ICANN's ability to perform the key ceremonies according to policy, due to global travel restrictions and guidance from governments and health authorities to limit gatherings of people.

Resolved (2020.12.17.xx), the Board finds the contingency plans continue to be in the best interests of ICANN and in the global public interest, and authorizes the President and CEO, or his designee(s), in consultation with the PTI President, to take all necessary steps to perform the key signing ceremonies as provided in the contingency plans during 2021.

PROPOSED RATIONALE:

1. Introduction

The Root Zone Key Signing Key (Root KSK) is managed using a system that deliberately disperses a number of trusted roles both logically and geographically as a security measure that is designed to reduce risk of collusion between parties to perform unplanned activity. In normal operations, many of these trusted role-players need to converge at one of two ICANN-managed sites (key management facilities, or KMFs) to perform "ceremonies" where each performs their role to perform essential KSK procedures, typically once every three months.

Due to the Coronavirus pandemic, ICANN org staff's mobility has been curtailed and other companies that supply these trusted roles have enacted similar policies. Further, governments have implemented travel restrictions that have a similar effect of reducing mobility. There is a significant risk that these

factors continue to impede the ability to hold key signing ceremonies in a normal manner. Without effective contingency plans, the inability to perform successful KSK operations would ultimately mean a widespread catastrophic failure of the DNS.

2. Board Remit

The Board's action on this matter is in-line with decision making it took in April 2020 at the beginning of the pandemic. This resolution seeks to extend the contingency plans beyond the period originally envisaged.

3. Proposal

The Board's action today is to authorize the President and CEO, in consultation with the PTI President, to continue to take all necessary steps to perform the key signing ceremonies as outlined in the following contingency plans. The ceremony management approach in the contingency plans continues to adapt ceremony operations to facilitate maximum safe participation and deciding upon alternatives where participation is not possible. It also provides for additional operational resiliency by performing signing operations for additional calendar quarters until ceremony operations can safely resume in their normal format.

The associated procedures and policies allow for operations in this format following adjustments adopted by ICANN's Policy Management Authority on 6 April 2020. In particular, the DNSSEC Practice Statement[1] (DPS) formally governs how KSK management is performed, and has been revised to allow for implementation of the presented options following proper authorization by management.

3.1 KSK Ceremony 42 (2021Q1)

Staff has taken lessons learned planning and conducting KSK Ceremony 41, improved details based upon community feedback, and proposes to perform KSK Ceremony 42 in a similar manner which satisfies the broader Internet

[1] https://www.iana.org/dnssec/dps

community and our DPS requirements. The ceremony would be held in the first quarter of 2021, with prospective attendees to be polled on the precise date upon adoption of this resolution.

3.1.1 Graduated set of options for ceremony performance

As with the 41st KSK ceremony held in April 2020, the final configuration of the ceremony will be held based on an assessment of the viability of a graduated set of options. These options provide for alternate mixes of personnel based on the nature of the restrictions around the time the ceremony is due to be held. In all cases, the ceremonies continue to be held in a public and transparent manner, with the ability for community members to participate remotely to assure confidence in how the ceremony is conducted. Compensative controls are effectively implemented to provide assurances regarding the custody of all secure elements used in the ceremony.

3.1.2 Signing for additional calendar quarters

The coronavirus pandemic is expected to continue to significantly impact operations well into 2021. To limit the impact on the ability to hold quarterly key ceremonies, the plan again provides for generating signatures for an extended nine month period. This relieves the need to hold a subsequent key signing ceremony until the fourth quarter of 2021.

3.2 KSK Ceremony 43 (2021Q4)

A successfully held ceremony in the first quarter of 2021, which generates nine months of signatures, would require the subsequent key ceremony to be held in the fourth quarter of 2021.

Staff will continue to monitor the pandemic and prepare for all possible scenarios for this ceremony in accordance with the graduated approach. Should widespread vaccination programmes prove to be successful, and international travel limitations be relaxed, it is conceivable a late-2021 ceremony could be conducted in its normal format with international in-person participation.

4. Stakeholder Consultation

The original contingency plan was developed in early 2020 through wide community engagement, including expected ceremony participants, the third-party auditor, the root zone maintainer, the vendors that support the key ceremony, the trusted community representatives and former ceremony attendees, ICANN's Root Zone Evolution Review Committee, and a number of relevant industry mailing lists. Subsequent to the April 2020 ceremony, the feedback received was universally positive that the modified format met the objectives and retained community trust in KSK management.

Many of these same parties have been apprised of our intention to extend the contingency plan into 2021 and have supported these efforts.

5. Fiscal Impact

This proposal is not anticipated to have a material fiscal impact beyond normal operational costs associated with KSK management.

6. Public Consultation Requirements

This matter relates to IANA Naming Functions operations, performed by PTI under contract from ICANN. Procedures that are used in KSK operations must be approved by the Policy Management Authority, an internal ICANN Org committee. There is no formal public comment requirement, however, IANA staff will continue to consult with the trusted community representatives and other stakeholders to implement and adapt these plans.

7. Public Interest

The Board's action is within the public interest and within ICANN's mission as it will help to continue to ensure the stable and secure operation of the Internet's unique identifier systems. The inability to conduct key signing ceremonies in a timely manner would result in widespread DNS resolution failure globally as

DNSSEC would cease to function. The Board's action will help ensure that DNSSEC-enabled devices will be able to resolve any domain names.

8. Key Risks

The following risk considerations were factored into the Board's deliberations on this action.

8.1 Travel of attendees is interrupted

The primary risk that this plan is designed to address is the inability of attendees to safely attend the key ceremony. The suggested mitigation is the graduated approach to different options to hold the ceremony, up to and including holding a ceremony only with staff in the Los Angeles metropolitan area, that will not require air or interstate travel, and with safety precautions for the individual attendees.

8.2 Facility operator suspends access to facility

The company that provides the facilities in which the KMFs are based may suspend access as part of their response to the pandemic. The suggested mitigation would be to advocate to their senior management, through trusted proxies if necessary, to make an exception given the requirement to hold this ceremony to support critical Internet infrastructure and Internet operation. ICANN has been in discussion with the US Government about issuance of special guidance should it be necessary to retain the access needed to perform the key ceremony.

8.3 Government suspends access to the facility, and/or constrains travel

Governments at different levels may impose restrictions on travel or gatherings that impede the ability to hold the ceremony. ICANN can advocate for exceptions to be made through the appropriate channels, as described in the previous section, noting the requirement to hold this ceremony to support critical Internet infrastructure and Internet operation. In particular, ICANN has

existing relationships with governments that can be used to seek such exemptions.

8.4 Staff become ill or otherwise indisposed

The minimum essential personnel may be incapable of performing the ceremony because they themselves are ill, quarantined or otherwise unavailable. The primary mitigation is PTI staff and other support staff from ICANN Org have been implementing social distancing since the beginning of March 2020 to limit potential transfer of illness. Additionally, there is approximately a three-month window to traverse the options presented, with sufficient slack to allow the exact date within each option to be adjusted to allow for recovery and still be held. There is also depth in staffing such that essential roles can be performed by different personnel if needed.

Signature Block:

Submitted by:	Kim Davies
Position:	Vice President, IANA Services; President, PTI
Date Noted:	14 December 2020
Email:	kim.davies@iana.org

REFERENCE MATERIALS – BOARD PAPER NO. 2020.12.17.1d

TITLE: **Contingency Plans for 2021 Key Signing Ceremonies**

1. Executive Summary

In early 2020, Key Ceremony procedures were adapted as a contingency measure in response to the COVID-19 pandemic. Limitations on travel and restrictions to bringing together personnel were key factors in modifying the approach, which normally brings together participants from throughout the world every three months.

We propose utilizing a similar approach for 2021 where normal ceremony operations are considered in light of the impacts of the pandemic on normal operations, using a graduated decision approach that would see ceremonies held in a restricted fashion until normal operations can safely resume.

2. Background

The Root Zone Key Signing Key (RZ KSK) is managed using a system that deliberately disperses a number of trusted roles both logically and geographically as a security measure designed to reduce risk of collusion between parties performing unplanned activity. In standard operations, many of these trusted role-players need to converge at one of two ICANN-managed sites (key management facilities, or KMFs) to perform "ceremonies" where individuals perform their role in essential KSK procedures, typically once every three months.

Due to the COVID-19 pandemic, since early 2020 ICANN org staff's mobility has been curtailed and other companies that supply these trusted roles are enacting similar policies. Further, governments have implemented travel restrictions that have a similar effect of reducing mobility. These limitations reduce available participation below our historical minimums and impact our ability to perform regular KSK management. Without effective contingency plans, the inability to perform successful KSK operations would ultimately mean a widespread catastrophic failure of the DNS.

2.1. KSK Ceremony 41 (2020 Q2)

Our most recent ceremony was held in April 2020 in a substantially modified fashion due to COVID-19 as follows:

- KSK Ceremony 41 was originally planned to be conducted as a standard ceremony on 23 April 2020 in the East Coast facility.
- In mid-February, recognizing the impact of COVID-19, the ceremony was significantly redesigned. A graduated set of options was devised, each one further deviating from standard operations. The graduated options were reviewed and endorsed by the ICANN Board.
- During preparation for the ceremony, the participants' ability to travel and the prevailing conditions relating to the COVID-19 pandemic were regularly monitored.
- The ceremony was held on 23 April 2020, but with minimum staff-only participation with four sets of trusted community representative credentials being couriered to LA for use in the ceremony.
- Ceremony activities were limited to only key signing operations. Additional activities to replace trusted community representatives and to induct a new hardware security module were deferred.
- Additional measures were adopted to bolster remote participation, allowing those who would normally be physically present to have an active role during the ceremony.
- Nine months of signatures were generated, but released in three month increments to Verisign. This was to defer the need for a subsequent ceremony during this period of uncertainty until 2021 Q1, while maintaining the standard signature release interval between cooperating parties.
- The public live stream had a greater than usual amount of interest and viewers.
- Ceremony was successful, and feedback was positive.

2.2. Reference Materials

- Questions and Answers on Coronavirus Mitigations https://data.iana.org/ksk-ceremony/41/KC41_qa.pdf
- ICANN Board resolution 2020.04.16.01 https://www.icann.org/resources/board-material/resolutions-2020-04-16-en

3. KSK Ceremony 42 (2021 Q1)

Staff has taken lessons learned planning and conducting KSK Ceremony 41, improved details based upon community feedback, and proposes to perform KSK Ceremony 42 in a similar manner which satisfies the broader Internet community and our DPS requirements.

Our main objectives are:

- Generation of required materials for continued DNSSEC operations
- Maintaining the health and safety of participants
- Security of the DNSSEC trust anchors
- Maintaining the confidence of the Internet community

KSK Ceremony 42 planning will be based upon our main objectives and several other factors:

Criteria for consideration for ceremony planning:

- Ensuring signatures do not expire in the DNS Root Zone (If the ceremony is not conducted by March 2021, DNSSEC validation would fail in April 2021)
- Coronavirus data/trends
- Government guidelines
- International and domestic flight availability
- Limits to freedom of movement (e.g. border and quarantine restrictions)
- Potential ceremony participants' willingness to participate

Decision authority to significantly modify operations:

- ICANN Board, ICANN President and CEO in consultation with the PTI President

Actions to minimize health risk associated with in-person KSK ceremony participation:

- Use of face covering and optionally other personal protective equipment
- Maintaining recommended physical distancing whenever possible
- Participants who feel sick, exhibit symptoms, test positive to COVID-19 or have otherwise been asked to quarantine cannot participate in the KSK ceremony physically, and will not be granted access to the secure facilities
- High risk individuals must consider their own personal safety

Additional considerations:

- Additional safety measures may be required to meet government regulations at the time of the KSK ceremony
- A recommended timeline will be established for each option and is subject to change based on global conditions at the time of implementation
- Proposed signature coverage and operations are based on evolving global pandemic conditions, future facility testing/maintenance, and subsequent ceremony timing

- Refer to Appendix A: Planned Scenarios for Holding a KSK Ceremony for additional information about planned scenarios

Table of Graduated Options for Holding KSK Ceremony 42

Due Date	Options	Suggested Signature Coverage	Suggested Operations
November 30, 2020	**Option A**: Hold the ceremony with a quorum of global participants	Standard ceremony that covers one calendar quarter (3 months)	Standard ceremony operations
	Option B: Hold the ceremony with only US-based participants in KMF East	Cover between one and four calendar quarters depending on best estimate on readiness for subsequent ceremony (3, 6, 9 or 12 months)	Hold the ceremony with a bare minimum of staff (7) and TCRs (3). Additional roles can be performed remotely
	Option C: Hold the ceremony in KMF West with only Los Angeles based personnel and minimum in-person participation		Hold the ceremony with a bare minimum of staff (7). TCR and additional roles can be performed remotely
March 1, 2021	**Move to option D**: Suspend signing of the DNS root zone if option C is not possible	N/A	N/A

3.1. Sign Key Materials Covering Additional Calendar Quarters

We propose implementing the same model as Key Ceremony 41, where additional calendar quarters are signed to guard against future near-term disruption.

A standard key ceremony generates signatures that cover one calendar quarter (3 months). In Ceremony 41, a decision was made to generate signatures that cover additional calendar quarters in this KSK ceremony to provide greater resilience to root zone operations during a period of ongoing uncertainty. Signatures covering future quarters are stored securely until transmitted, with the last set of signatures scheduled for transmission in November 2020.

The number of quarters signed can be increased or decreased to accommodate forecasted conditions, and in consideration of future ceremony maintenance and timing.

3.2. KMF Selection

There are two KMFs: KMF West located in El Segundo, California and KMF East located in Culpeper, Virginia. These two KMFs are duplicates of one another and either can be used, although normally we alternate between facilities with every key ceremony.

KMF East presents two challenges for holding this ceremony:

1. A lack of on-site personnel that can perform ceremonies without long-distance travel
2. Culpeper, VA weather conditions[1] at that time of year can result in a localized inability to travel to the facility. Attendees to previous ceremonies at this time of year have not been able to reach the facility due to snow and ice.

As a consequence, we propose using KMF West for this ceremony. Recognizing this extends the period in which KMF East's facility has not been exercised or maintained, planning is underway to perform equipment maintenance and testing in KMF East later in 2021 distinct from Ceremony 42. This will also allow COVID-19 pandemic conditions and preparedness to improve so staff may more safely travel to perform equipment maintenance and testing before resuming key ceremonies in KMF East.

[1] December, January and February are the frosty months with average temperature fluctuating between 45 F (7.2 C) and 25 F (-3.9 C). https://www.weather-us.com/en/virginia-usa/culpeper-climate

4. KSK Ceremony 43 Forecasting

Future ceremony planning needs to continue to consider the COVID-19 pandemic and adapt accordingly. Currently, U.S. health officials estimate that widespread vaccines could be available 2021 Q2[2], which if realized would improve the opportunity to start resuming normal ceremony operations in the second half of 2021. It is anticipated that ceremony attendees will avail themselves of vaccinations when available. Should key staff be able to receive vaccinations in this time frame, it should allow for safe travel to perform testing and deferred maintenance in KMF East during 2021 Q3. Such maintenance should allow for any necessary testing and remediation to be performed in preparation for a KMF East ceremony in 2021 Q4.
According to these factors, with the most likely estimate for a subsequent key ceremony in 2021 Q4, it would suggest that the 2021 Q1 key ceremony should generate signatures for three calendar quarters.

5. KMF East Risk Mitigation Plan

Due to risks associated with travel and gathering in the current pandemic climate, KMF East is experiencing an extended period of inactivity. This section addresses the key risks we've identified with an extended period of inactivity in KMF East, and provides a plan to mitigate these risks before performing another key ceremony in KMF East.

5.1. KMF East Key Risks

The following list represents the key identified risks and their mitigations:

Risk: *HSMs fail to perform cryptographic operations due to battery failure*

Mitigation: There are currently five production HSMs spanning two facilities, plus additional backups that can be activated by the disaster recovery process. Two production HSMs reside in KMF East, with another new HSM pending introduction. Each HSM contains dual batteries. These batteries are required to safeguard the contents of the HSM in a powered down state. The anticipated shelf life of the battery is approximately 10 years. The failure rate of two batteries in a single HSM is easily mitigated by the redundancy of multiple HSMs. Each unit reported their battery condition as good in 2019 and/or 2020. Detailed HSM information can be found in the equipment section of this document.

In the highly unlikely scenario that both HSMs in KMF East are not able to perform cryptographic operations, utilizing Recovery Key Share Holders in KMF East or generating the necessary materials to recover KMF East in KMF West would both be possible. Future plans to reissue CO credentials (which

[2] Dr. Fauci's most recent conference including a COVID-19 vaccine timeline https://www.msn.com/en-us/news/us/fauci-tells-congress-it-might-take-some-time-before-the-public-gets-a-coronavirus-vaccine/ar-BB19lDWe

include issuing additional HSM smartcards) would further streamline this scenario, allowing recovery solely in KMF East with its assigned Crypto Officers.

Risk: *KMFs infrastructure failure: undetected equipment malfunction due to inactivity*

Mitigation: The KMFs are constantly monitored by two independent and concurrent systems, and are well protected by overlapping tiers of systems and security. Daily heartbeat monitoring and overlapping intrusion detection systems ensure any malfunction is quickly detected. A procedure has been developed which will ensure all equipment is thoroughly inspected, tested, and remediated if necessary prior to the next KMF East KSK ceremony.

Additionally, the IDS-ACS (Intrusion Detection System-Access Control System) and video surveillance systems for both KMFs can be accessed and tested from either facility.

Risk: *KMF East Safe #2 (Credentials Safe) lock failure: Safe fails to open*

Mitigation: KMF East Safe #2 (Credentials Safe) is equipped with a Kaba-Mas X-09 safe lock. The Kaba-Mas X-09 has reached end of life and has been superseded with the Kaba-Mas X-10 by its manufacturer.

The Kaba-Mas X-09 is scheduled to be replaced for a Kaba-Mas X-10 well before the next KSK Ceremony in the KMF East, allowing ample time for remediation if necessary.

In a scenario where the KMF East Safe #2 (Credentials Safe) safe lock will not open, a trained locksmith will drill the safe and replace the safe lock with a Kaba-Mas X-10.

Risk: *Both laptops at KMF East experience equipment failure*

Mitigation: While this is highly unlikely, a new spare ceremony laptop is in the possession of RKOS and will be made available.

5.2. Mitigation Plan

Maintenance and testing will be performed in KMF East well ahead of any scheduled KSK ceremony. This process will include the following activities:

- Replacement of Safe #2 (Credentials Safe) Kaba-Mas X-09 with a Kaba-Mas X-10
    - Ideally performed with one or more in-person TCR witnesses
- Replacement of five safe deposit box lock assemblies in Safe #2 (Credentials Safe)
- Maintenance and testing of the IDS-ACS (Intrusion Detection System-Access Control System)
- Testing HSMs to check their battery levels and ensure there is no tamper indication
- Video surveillance server and camera testing and maintenance
- Testing and maintenance of Audiovisual equipment required for live streaming

5.3. Equipment

1. **HSM(s)**
   Ultra Electronics Keyper Plus HSMs are currently used in the KSK production environment. These HSMs are equipped with batteries which protect the cryptographic keys when they are powered down. The batteries have a manufacturer's shelf life of 10 years. The HSM manufacturer's recommendation is to replace the batteries every 5 years. Battery replacement must be performed by the manufacturer at their facility, which is not an option for the KSK production environment. Complete loss of battery power would result in a positive tamper and an inability to access the cryptographic keys stored in the HSM. Our current rationale is to target a life cycle approximate to 4 years; well within the manufacturer's recommended battery life.

   The following table summarizes the current production HSMs:

KMF	HSM	Battery Manufacture Date	Introduction Date	Last Used Date - Status
West	**HSM3**	July 2013	13 August 2015	16 February 2020 - OK
	HSM4	February 2014	13 August 2015	16 February 2020 - OK
	HSM5W	March 2019	14 August 2019	23 April 2020 - OK
East	**HSM4**	February 2014	9 April 2015	14 November 2019 - OK
	HSM5E	March 2019	16 May 2019	16 May 2019 - OK

HSM6E has been procured and is pending introduction in KMF East, scheduled for the next east coast key ceremony. HSM6W will be purchased and introduced at the next standard KMF West KSK ceremony.

2. **HSM Smartcards (CO Credentials)**
   The HSM smartcards are the original smartcards issued in 2010. The already infrequent usage of the HSM smartcards suggests the period of inactivity will not have adversely affected their functionality. Previously, SO cards have experienced multiple years without use and exhibited no issues.

   There is a plan to regenerate and replace the CO smartcard credentials previously communicated which will replace the original smartcards and provide greater disaster recovery options and assist in streamlining future key ceremonies.

3. **Ceremony Laptop(s)**
   Currently there are two laptops in production at KMF East. We do not anticipate any appreciable risk associated with the period of inactivity. We do however have a new backup ceremony laptop that could be made available.

4. **ACS-IDS (Access Control System and Intrusion Detection System)**
   The ACS-IDS consists of two independent systems constantly and actively monitoring both KMFs. Any failure would be detected by a lack of regular heartbeat indications from the ACS-IDS or a telephone call from our security monitoring vendor. The ACS-IDS for both KMFs can be accessed and tested from either facility. The ACS-IDS will be tested and exercised prior to the next upcoming KMF East key ceremony.

5. **Video Surveillance System**
   Real time monitoring ensures that the video surveillance server is operational. The video surveillance systems for both KMFs can be accessed and tested from either facility. Additionally, constant video surveillance is provided by the Equinix facility.

6. **Safe Locks/Dials**
   KMF East has a Kaba-Mas X-10 dial in Safe #1 (Equipment Safe), and a Kaba-Mas X-09 dial in Safe #2 (Credentials Safe). The already infrequent usage of the safe dials suggests the period of inactivity will not have adversely affected their functionality. The X-09 safe dial is scheduled to be replaced prior to the next upcoming KMF East key ceremony.

7. **Audiovisual equipment**
   The already infrequent usage of the audiovisual equipment suggests the period of inactivity will not have adversely affected its functionality. All audiovisual equipment will be tested and exercised prior to the next upcoming KMF East KSK ceremony.

6. Questions and Answers

When will standard key ceremonies resume?

As soon as they can be safely conducted with the necessary global in-person participation. Future key ceremony planning will be informed by the evolving COVID-19 pandemic, global health advisories, travel and visa restrictions, and participants' willingness to travel and attend key ceremonies. We currently believe 2021 Q4 is the earliest we anticipate a standard ceremony may be possible.

Two Crypto Officers based at KMF East were scheduled to retire at KSK Ceremony 41 before the ceremony was moved to KMF West. How has the situation evolved?

We continue to speak with our community volunteers, including these two Crypto Officers, to understand their constraints and requirements. Both retiring COs have indicated to us their willingness to remain in their roles until another in-person KSK ceremony is possible, ensuring an optimal transition.

When will the next KSK Rollover occur?
We do not plan to generate a new KSK under our modified ceremony procedures unless necessary (e.g. an emergency rollover). Therefore, the earliest anticipated opportunity to generate a future KSK would be when we return to standard KSK ceremony operations.

7. Appendix A: Planned Scenarios for Holding a KSK Ceremony

The graduated approach consists of four options, ranked from most desirable to least desirable. Each has associated conditions and approval processes for moving to the next option:

7.1. Option A: Hold the Ceremony With a Quorum of Participants Globally.

The ceremony can continue to be held according to normal procedure if the minimum number of attendees are present, including a minimum of Trusted Community Representatives (TCRs).

Ceremony Operation:

- Standard ceremony procedure will proceed with extraneous acts
- Full quorum of participants
- Single calendar quarter of signatures generated

Key risks: Holding the ceremony as planned relies on international mobility of TCRs which is currently severely compromised, and the future evolution of these restrictions is unpredictable. Staff mobility is also impacted domestically.

Proceeding to Option B: If in the judgment of the President of PTI the situation does not stabilize with a high-level of confidence the ceremony can be held as scheduled, Option B shall become the preferred option.

7.2. Option B: Hold the Ceremony With Only US-based Personnel

Three of the seven TCRs for the Culpeper location are based in the US, two on the east coast and one on the west coast.

Only one of the seven TCRs for the El Segundo location is based in the US, on the east coast.

There are qualified ICANN staff based out of the Los Angeles (LA) and Washington (DC) ICANN offices.

Ceremony Operation:

- Focused ceremony procedures for signature generation excluding nonessential acts
- US-based TCRs and staff in attendance only
- One or two calendar quarters of signatures generated
- Can only take place in KMF East with currently active TCRs

Key risks: This option relies upon ongoing domestic mobility of trusted community representatives and staff. It also assumes necessary personnel do not get sick or otherwise cannot attend, as there is no safety margin for non-attendance.

Proceeding to Option C: If in the judgment of the President of ICANN the ceremony cannot be committed to with a high level of confidence or otherwise cannot be executed as scheduled, Option C becomes the preferred option.

7.3. Option C: Hold the Ceremony With Only Los Angeles Based Personnel and Minimum In-Person Participation

The Key Management Facilities (KMFs) were expressly designed to allow for staff-only ceremonies in a disaster recovery ceremony to ensure key ceremonies are held as needed. The minimum essential personnel could perform a key ceremony in our El Segundo KMF on short notice. This would, however, not have the required number of trusted community representatives present in-person.

Ceremony Operation:

- Focused ceremony procedures for signature generation excluding nonessential acts
- US-based staff only in attendance
- Use 3 TCRs' credentials, either by having their access keys transmitted to US-based surrogates securely in advance of the ceremony, or by drilling the safety deposit box that holds their secure credentials
- Conduct the ceremony with typical audit coverage and live streaming to allow interested parties to witness, and additionally providing opportunities for TCRs and other key parties to actively participate in the ceremony remotely
- One, two, three, or four calendar quarters of signatures generated

Key risks: This option requires a minimum number of staff and contractors to be available (i.e. not incapacitated or restricted in movement). It breaches the standard expectations on participation in key ceremonies, but is considered an option within scope of the disaster recovery procedure.

Proceeding to Option D: If the ceremony cannot be conducted by the end of the quarter or before DNSSEC signature expiration, Option D becomes the ultimate option. The Board of ICANN shall make the final determination to move to Option D.

7.4. Option D: Suspend Signing of the DNS Root Zone

This is the final option if there is no conceivable way to activate the KSK and perform signing operations. There would need to be a massive education campaign at short notice to have resolver operators disable

DNSSEC validation. There is a high risk of widespread outages as it is not possible to ensure global implementation, and high risk this will fatally compromise trust in DNSSEC in general as a technology.

This is considered highly unlikely, but nonetheless the final option. Without exercising the option, in the absence of a successful key signing ceremony, DNSSEC validation would be unsuccessful starting in the next quarter after DNSSEC signature expiration.

Required Operations and Anticipated Impact:

- Suspend signing of the DNS root zone
- Significant outreach to DNS operators and broader Internet community required
- Anticipated widespread and catastrophic failure of the DNS

8 December 2020

ICANN BOARD SUBMISSION No. 2020.12.17.1e

TITLE: **Change to Service Agreement,** Confidential Negotiation Information

PROPOSED ACTIONS: **For Board Consideration and Approval**

EXECUTIVE SUMMARY:

The Board is being asked to approve a new contract for the processing of payments by credit cards supported by the provider, Confidential Negotiation Information
Confidential Negotiation Information

Accordingly, Board approval is required in accordance with ICANN's Contracting and Disbursement Policy.

ICANN is expected to realize these savings through a new contract Conf dent a Negot at on Informat on Confidential Negotiation Information The new contract provides more qualification categories by card type. ICANN will also improve on this process by offering the stakeholders a self-service portal that eliminates the need for transferring personal data via facsimile. Confidential Negotiation Informa selected over other participants as it provides the most cost savings and best product value.

ICANN ORGANIZATION AND BOARD FINANCE COMMITTEE (BFC) RECOMMENDATION *(Subject to BFC approval):*

ICANN organization recommends that the Board authorizes the President and CEO, or his designee(s), to take all necessary actions to execute a new contract with Confidential Negotiation Informati and to make all necessary disbursments pursuant to the contract.

PROPOSED RESOLUTION:

Whereas, ICANN has established a need to enter into a new contract for the processing of credit card payments, supported by Confidentia Negotiation nformation

Whereas, the Board Finance Committee has reviewed the financial implication of contracting with Confidential Negotiation nformation

Whereas, both the organization and the Board Finance Committee have recommended that the Board authorize the President and CEO, or his designee(s), to take all actions necessary to execute the new contract Confidential Negotiation Informati and to make all necessary disbursments pursuant to the contract.

Resolved (2020.12.17.xx) the Board authorizes the President and CEO, or his designee(s), to take all necessary actions to execute a new contract with Confidential Negotiation Informatio and to make all necessary disbursments pursuant to the contract.

Resolved (2020.12.17.xx), specific items within this resolution shall remain confidential for negotiation purposes pursuant to Article 3, section 3.5(b) of the ICANN Bylaws until the President and CEO determines that the confidential information may be released.

PROPOSED RATIONALE:

ICANN org has partnered with Confidential Negotiati for the processing of credit card payments since September 2007. Over the years, the volume of payments that ICANN receives by credit cards has increased and the tiered rate structure negotiated in 2007 is no longer favorable to ICANN. However, ICANN wishes to continue offering this convenient method of payment to its stakeholders through its longtime partner and reputable service provider, Confidential Negotiation nformation

ICANN determined that under a new rate structure, Confidential Negotiati provided the most cost savings and best product value following a formal Request for Proposal (RFP) to identify potential service providers against 10 nominees and three participants.

As an established partner, Confidential Negotiation offers minimal transition efforts and a good history of transferring funds between the issuing bank and ICANN, without delays or disputes. Confidential Negotiati also meets our three primary objectives:

1. Secure services that meet global and local laws and regulations.
2. Reduce ICANN's cost associated with credit card merchant fees.

3. Migrate to a payment gateway service, increasing efficiency and accuracy for payments received by credit card.

Rationale Text Superseded

ICANN has also negotiated favorable terms. The initial term of the new contract is three years with an automatic one-year renewal period. The contract can be canceled at any time with 60-days advance notice. Confidential Negotiation Informa fees are fixed for the contract term and will not increase.

After careful analysis, the Board agrees with the organization that the new contract is a more cost-effective solution for offering payments by credit cards at this time. The Board understands that the organization will continue to review other payment alternatives to further reduce the expense associated with these services and it will implement a process of regularly reviewing the fees billed by the service provider.

Executing the contract on favorable terms is in the public interest as it will lower ICANN's expenses without any impact to the services ICANN provides to its community and therefore is also consistent with ICANN's Mission.

There is a positive fiscal impact in that the new contract will result Rationale Text Superseded . There is no anticipated impact to the security, stability, and resiliency of the domain name system.

This is an Organizational Administrative function that does not require public comment.

Submitted by: Xavier Calvez, SVP, Planning and Chief Financial Officer
Date Noted: 3 December 2020
Email: xavier.calvez@icann.org

8 December 2020

ICANN BOARD PAPER NO. 2020.12.17.2a

TITLE: **2020 Strategic Outlook Trends Report**

PROPOSED ACTION: **For Board Consideration and Approval**

EXECUTIVE SUMMARY:

Tracking new and shifting trends affecting ICANN and the Internet is a critical first step in ICANN's strategic planning process. The Board Strategic Planning Committee oversees the annual strategic outlook (trends) process to identify relevant trends and events that inform ICANN's strategic planning and prioritization efforts and the annual review of the Strategic Plan.

This year, ICANN org convened 21 Strategic Outlook trends identification sessions with 398 participants from the community and the organization, resulting in 1,853 data points collected. The Board Strategic Planning Committee, supported by ICANN org, conducted a thorough analysis of the trend session data inputs received, including assessing the trends, risks, opportunities, and potential impacts on ICANN.

A description of the Strategic Outlook process and methods used to conduct the analysis, the results of those analyses, and appendices with more details on the trend inputs received have been documented in the *2020 Strategic Outlook: Trend Synthesis* document attached to this paper for reference. The process and methods used were shared with the community during a webinar held on 06 October 2020.

The synthesis of this analysis is a set of proposed priority trends, related impacts, and associated strategic and/or tactical recommendations, summarized in the table below.

With new five-year plans just coming into effect in July of this year, little to no changes were expected. The assessment made of this year's strategic outlook trends focused, in particular, on evaluating potential short- and/or long-term impacts of the coronavirus pandemic on ICANN's plans. On the basis of the analysis to-date some adjustments to the Operating Plan have been identified, but the strategic objectives of the organization at this point do not need to change.

The Board is now being asked to consider these recommendations and to confirm that the current ICANN Strategic Plan for Fiscal Years 2021-2025 remains unchanged.

As next steps, ICANN org will take in consideration the recommendations listed below when drafting the ICANN Five-year Operating Plan for Fiscal Years 2022 to 2026. Findings on trends and their impacts on ICANN, as well as opportunities they represent and resulting proposed planned activities, will be documented in the next ICANN Operating Plan that will be posted for Public Comment in December of this year. Finally, the proposed 2020 trends will serve as reference for the next iteration of the Strategic Outlook trends identification process, which will start early 2021 at the latest.

SUMMARY OF TRENDS, IMPACTS AND RECOMMENDATIONS

2020 Trend Proposal	Shift in trend	Impacts on ICANN	Conclusions & Actions Taken
On Security: DNS ecosystem secur ty threats rema n h gh and have the potent a to erode the pub c trust n ICANN s ab ty to fu f ts m ss on.	Increased reputat ona r sk nherent to the ack of understand ng of ICANN s ro e	Cont nued he ghtened secur ty threats are erod ng pub c percept on about the ntegr ty of the system, potent a y hamper ng ICANN's ab ty to fu f ts m ss on.	Opportun ty to a gn percept ons and draw a d st nct on between DNS ecosystem secur ty threats and DNS Abuse; to create awareness of the d fferences between the two and magn tude of each; and to exp a n ICANN s ro e n address ng DNS secur ty threats. (Cons dered n Operat ng P an; no change n Strateg c P an)
On Security: There s ncreas ng pressure from the commun ty for ICANN to address "DNS abuse" ssues; however, quest ons rema n – w th no c ear consensus – about what const tutes "DNS abuse", and about what ICANN s ro e shou d be n re at on to "DNS abuse".	Increased pressure to address "DNS abuse"	Increases n "DNS abuse" are affect ng user secur ty, hav ng an mpact on ICANN s cred b ty, and mak ng the Internet untrustworthy.	Opportun ty for commun ty to a gn on what const tutes DNS abuse and what ICANN's ro e shou d be n combat ng abus ve use of the DNS (Cons dered n Operat ng P an; no change n Strateg c P an)
On ICANN's Governance: COVID-19 pandem c-re ated d srupt on s acce erat ng commun ty's nterest to evo ve ICANN s mu t stakeho der mode to be ag e n the face of change and to support equ tab e, eff c ent processes for effect ve dec s on-mak ng.	Commun ty part c pat on concerns exacerbated by pro onged v rtua sett ngs (nab ty to meet face-to-face)	Reduced or nsuff c ent commun ty part c pat on cou d s ow down commun ty s work and r sks capture and threat to ICANN s mu t stakeho der mode due to oss of trust, cred b ty, and eg t macy.	Opportun ty to evo ve both the ICANN pub c meet ngs strategy and the p ann ng and mp ementat on of the work on Enhanc ng the Effect veness of ICANN's Mu t stakeho der Mode (Cons dered n Operat ng P an; no change n Strateg c P an)

2020 Trend Proposal	Shift in trend	Impacts on ICANN	Conclusions & Actions Taken
On Geopolitics: There s an ncreased effort by nat ona and reg ona governments as we as ntergovernmenta organ zat ons and other types of n t at ves to regu ate or eg s ate the Internet. Th s trend has the potent a to ead to act ons threaten ng the operab ty and openness of the Internet and ncreases the comp ex ty of ICANN operat ons and po cy deve opment.	The COVID-19 pandem c has moved more spheres of fe on ne	The COVID-19 pandem c ncreases the r sk of governmenta ntervent ons due to the ncreased percept on of Internet and Internet-based serv ces as essent a ut t es. The push to a mu t atera mode of Internet governance s an ex stent a threat for ICANN s mu t stakeho der mode . Mu t p e r sks assoc ated w th the ncrease n nat ona eg s at on and regu at ons.	Cont nue bu d ng understand ng at the nat ona /reg ona /IGO eve about the techn ca way the Internet funct ons, and w th n that what s ICANN s ro e n ma nta n ng a stab e g oba y nteroperab e Internet. Rema n engaged n d scuss ons about Internet governance nc ud ng engagement and educat ona outreach to IGOs and other ent t es, d scuss ng ssues that may touch upon ICANN s m ss on n order to ncrease understand ng and awareness of potent a un ntended negat ve consequences to the nteroperab e s ng e Internet. Mon tor add t ona arenas that are d scuss ng eg s at ve, regu atory, or IGO reso ut ons and expand engagement nto these add t ona governmenta arenas. (Cons dered n Operat ng P an; no change n Strateg c P an)
On Financials: The eve of r sk for ICANN s ong-term fund ng s ncreas ng n the face of changes n the marketp ace, deve opments around the expans on of the gTLD name space, and the onset of a g oba recess on/depress on.	Onset of g oba recess on	Fund ng mode s based so e y on numbers of reg strat ons may not be susta nab e n a recess on (not ng that th s mpact has not yet mater a zed.)	No add t ona act on bes des the dec s on that was a ready made n May 2020 to de ay FY21 Operat ng n t at ves requ r ng ncrementa resources to FY22. Cont nue to mon tor c ose y and reassess the r sk regu ar y. (No changes to strateg c or operat ng p ans)
On Unique Identifier Systems: The rap d evo ut on of emerg ng dent f er techno og es requ res ICANN to be respons ve to these changes and ensure that the un que dent f er systems evo ve and cont nue to serve the g oba Internet user base.	No notab e sh fts, ast year s trends rema n true	No new mpacts	No changes to strateg c or operat ng p ans

BOARD STRATEGIC PLANNING COMMITEE RECOMMENDATION:

The Board has an obligation for ensuring that the adopted Strategic Plan for Fiscal Years 2021-2025 continues to meet ICANN's needs. The Board Strategic Planning Committee, as supported by the ICANN organization, recommends keeping the ICANN Strategic Plan for fiscal years 2021 to 2025 unchanged, with no restatement of the

Strategic Plan needed at this time. This recommendation is formed on the basis of the work accomplished by the Strategic Planning Board Working Group in place prior to the formation of said committee, and after careful consideration of the inputs received from the community and the organization through the Strategic Outlook trends identification process. The Board Strategic Planning Committee recognizes that there may be future needs to evolve the Strategic Plan, such as to address funding realities identified through the update of ICANN's five-year Operating and Financial plan, or mid-course modifications during the life of the Strategic Plan. If change is needed in the future, the Board can direct the ICANN org on the scope of further actions.

PROPOSED RESOLUTION:

Whereas, following community and ICANN organization inputs received between November 2019 and March 2020 on key trends anticipated to impact ICANN in the coming years, the Board conducted an analysis, and concluded that the strategic objectives for ICANN, as reflected in the Strategic Plan for Fiscal Years 2021-2025, do not need to change.

Whereas, on 22 October 2020, the Board formed a Strategic Planning Committee to oversee the annual strategic outlook (trends) process to identify relevant trends and events that inform ICANN's strategic planning and prioritization efforts. Prior to that date, the Board relied upon the use of a Board Working Group on Strategic Planning. This working group, as supported by ICANN organization, played a central role in reviewing and analyzing the results of the trend work and the related opportunities, risks, and impacts on ICANN. The working group articulated this work into a set of proposed priority trends, related impacts, and associated strategic and/or tactical recommendations for full-Board consideration.

Whereas, members of the ICANN Board and ICANN organization held a webinar with the community on 06 October 2020 to present the Strategic Outlook process and methods used to conduct the analysis.

Resolved (2020.12.17.xx), the Board affirms that the ICANN Strategic Plan for Fiscal Years 2021 to 2025 shall remain in force and unchanged, with no restatement of the Strategic Plan needed at this time.

Resolved (2020.12.17.xx), the Board recognizes that there may be future need to evolve this Strategic Plan, such as to address funding realities identified through the update of ICANN's five-year Operating and Financial plan, or mid-course modifications during the life of the Strategic Plan. If change is needed, the Board will direct the ICANN org on the scope of further actions.

PROPOSED RATIONALE:

On 23 June 2019, the Board adopted the ICANN Strategic Plan for Fiscal Years 2021 to 2025 and directed that as part of the on-going annual planning cycle with the community, new trends or shifts in existing trends be factored into the annual iteration of ICANN's plans as appropriate. These efforts are conducted under a process known as the Strategic Outlook trend identification process.

The Strategic Outlook trend identification is an annual process, which ensures ICANN has a consistent way to: identify and track trends; prepare for opportunities; mitigate or avoid challenges; inform strategic and operational planning and prioritization.

It is a joint effort between the ICANN organization, the community, and the ICANN Board to engage on emerging or evolving trends that affect ICANN. Trends indicate general directions in which things are developing or changing, that have or could have an impact on ICANN, its mission, its operations, or its ecosystem. Trends can be internal or external, organization-specific, community-related, or go beyond ICANN's ecosystem as ICANN does not operate in a vacuum.

The ICANN org has found the exercise to be beneficial to help surface opportunities and challenges that lay ahead, inform planning, help with prioritization considerations, and risk management.

Between November 2019 and March 2020, ICANN org convened 21 Strategic Outlook trends identification sessions with 398 participants from the community and the

organization, resulting in 1,853 data points collected. Community sessions outputs have been published on the Strategic Planning page of the icann.org website.

Between April and September 2020, the Strategic Planning Board Working Group, as supported by ICANN org, conducted a thorough analysis of the trend session data inputs received, including assessing the trends, risks, opportunities, and potential impacts on ICANN. The details of this analysis and associated recommendations have been documented in the *2020 Strategic Outlook Trends Report* document attached to this paper for reference.

The Board Strategic Planning Committee, on the basis of the work accomplished by the Strategic Planning Board Working Group in place prior to the formation of the committee, recommends keeping the ICANN Strategic Plan for Fiscal Years 2021 to 2025 unchanged, with no restatement of the Strategic Plan needed at this time.

This resolution is not expected to have a fiscal impact on ICANN, though the changes anticipated to ICANN's Operating Plan might have impact once approved. This action is expected to should have a positive impact on the security, stability and resiliency of the domain name system (DNS) as it continues to support ICANN's strategic work in this area.

This resolution serves ICANN's mission in ensuring a secure and stable operation of the Internet's unique identifier systems. The ICANN Strategic Plan for Fiscal Years 2021-2025 builds upon ICANN's mission so that it may continue to effectively fulfil its aims and meet new and continuously evolving challenges and opportunities.

This resolution is in the public interest as the Strategic Plan guides ICANN's activities and informs ICANN's operating plans and budgets to fulfil its mission in fiscal years 2021 through 2025. The Strategic Plan serves the public interest by articulating the path towards a new vision to be a champion of the single, open, and globally interoperable Internet. The Strategic Plan complies with ICANN's commitments and is guided by ICANN's core values.

This is an Organizational Administrative Function that has been subject to community consultation as noted above, and is not requiring further public comment.

REFERENCE MATERIALS: 2020 Strategic Outlook Trends Report

Signature Block:

Submitted by:	Matthew Shears
Position:	Member of the ICANN Board, Chair of the Board Strategic Planning Board Committee
Date Noted:	XX November 2020
Email:	matthew.shears@board.icann.org

ICANN Strategic Outlook: 2020 Trends Report

[Subject]

ICANN Planning Department
13 November 2020

ICANN

TABLE OF CONTENTS

1 Executive Summary

Tracking new and shifting trends affecting ICANN and the Internet is a critical first step in ICANN's strategic planning process. Each year, ICANN utilizes trend information to inform appropriate changes to the ICANN five-year strategic plan, operating plans (five-year or annual), and budget. This paper provides a summary of ICANN's 2020 strategic outlook process, a bottom-up process to identify trends and their impacts on ICANN. It is intended to inform the community, Board, Executive Team, and relevant ICANN staff about shifts in trends that may affect their work, planning, and budget.

In 2020, ICANN convened 21 strategic outlook sessions with 398 participants resulting in 1,853 data points collected. Trend session participants were asked to consider trends, risks, and opportunities across five focus areas: Security, Unique Identifier Systems, Governance, Geopolitics, Financials.

This year, discussions within the org also included a sixth focus area on Operational Excellence.

Related results will serve as input for org's on-going organizational assessment and continuous improvements efforts, and are included in Appendix C.

Trend session data inputs received go through a thorough analysis including assessing the trends, risks, opportunities, and potential impacts on ICANN. The synthesis of this analysis is a set of proposed priority trends, related impacts, and associated strategic and/or tactical recommendations, summarized in the table below.

This paper also provides a description of the Strategic Outlook process and methods used to conduct the analysis, the results of those analyses, and appendices with more details on the trend inputs received.

SUMMARY OF TRENDS, IMPACTS AND CONCLUSIONS

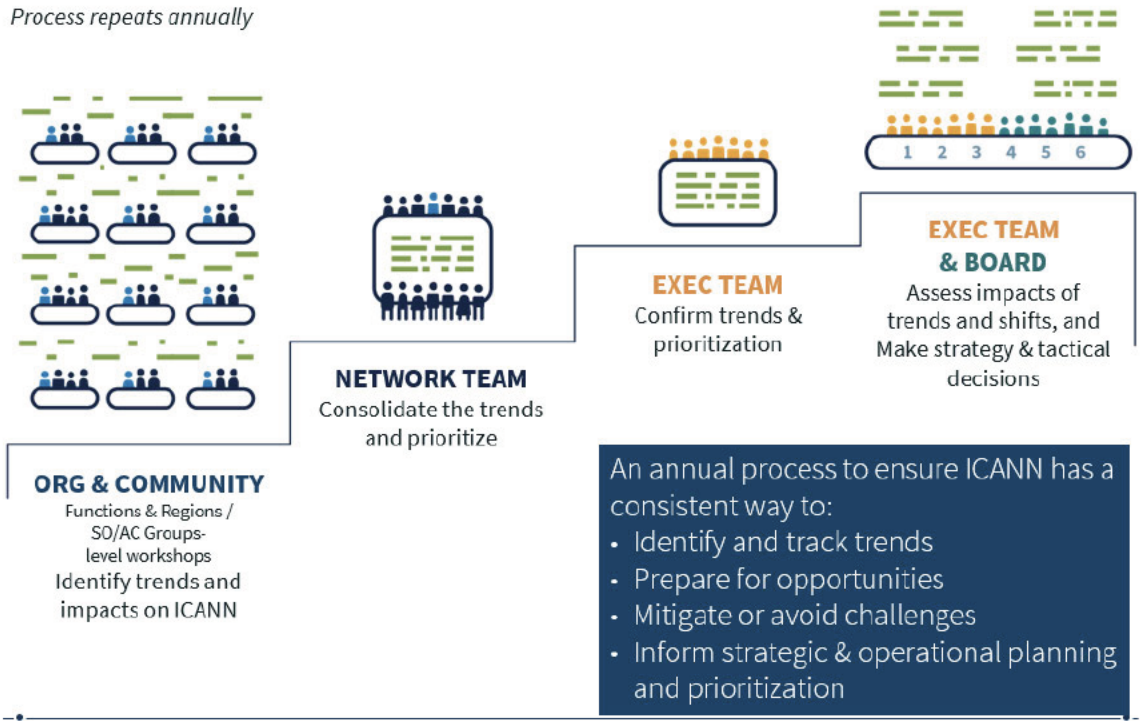
With new five-year plans that just came into effect in July of this year, little to no changes were expected to ICANN plans at this time. The assessment made of this year's strategic outlook trends focused, in particular, on evaluating potential short- and/or long-term impacts of the coronavirus pandemic on ICANN's plans. On the basis of the analysis to-date, some adjustments to the Operating Plan have been identified (see table below), but the strategic objectives of the organization at this point do not need to change.

2020 Trend Proposal	Shift in trend	Impacts on ICANN	Conclusion & Actions Taken
On Security: DNS ecosystem secur ty threats rema n h gh and have the potent a to erode the pub c trust n ICANN s ab ty to fu f ts m ss on.	Increased reputat ona r sk nherent to the ack of understand ng of ICANN s ro e	Cont nued he ghtened secur ty threats are erod ng pub c percept on about the ntegr ty of the system, potent a y hamper ng ICANN's ab ty to fu f ts m ss on.	Opportun ty to a gn percept ons and draw a d st nct on between DNS ecosystem secur ty threats and DNS Abuse; to create awareness of the d fferences between the two and magn tude of each; and to exp a n ICANN s ro e n address ng DNS secur ty threats. (Cons dered n Operat ng P an; no change n Strateg c P an)
On Security: There s ncreas ng pressure from the commun ty for ICANN to address "DNS abuse" ssues; however, quest ons rema n – w th no c ear consensus – about what const tutes "DNS abuse", and about what ICANN s ro e shou d be n re at on to "DNS abuse".	Increased pressure to address "DNS abuse"	Increases n "DNS abuse" are affect ng user secur ty, hav ng an mpact on ICANN s cred b ty, and mak ng the Internet untrustworthy.	Opportun ty for commun ty to a gn on what const tutes DNS abuse and what ICANN's ro e shou d be n combat ng abus ve use of the DNS (Cons dered n Operat ng P an; no change n Strateg c P an)
On ICANN's Governance: COVID-19 pandem c-re ated d srupt on s acce erat ng commun ty's nterest to evo ve ICANN s mu t stakeho der mode to be ag e n the face of change and to support equ tab e, eff c ent processes for effect ve dec s on-mak ng.	Commun ty part c pat on concerns exacerbated by pro onged v rtua sett ngs (nab ty to meet face-to-face)	Reduced or nsuff c ent commun ty part c pat on cou d s ow down commun ty s work and r sks capture and threat to ICANN s mu t stakeho der mode due to oss of trust, cred b ty, and eg t macy.	Opportun ty to evo ve both the ICANN pub c meet ngs strategy and the p ann ng and mp ementat on of the work on Enhanc ng the Effect veness of ICANN's Mu t stakeho der Mode (Cons dered n Operat ng P an; no change n Strateg c P an)
On Geopolitics: There s an ncreased effort by nat ona and reg ona governments as we as ntergovernmenta organ zat ons and other types of n t at ves to regu ate or eg s ate the Internet. Th s trend has the potent a to ead to act ons threaten ng the operab ty and openness of the Internet and ncreases the comp ex ty of ICANN operat ons and po cy deve opment.	The COVID-19 pandem c has moved more spheres of fe on ne	The COVID-19 pandem c ncreases the r sk of governmenta ntervent ons due to the ncreased percept on of Internet and Internet-based serv ces as essent a ut t es. The push to a mu t atera mode of Internet governance s an ex stent a threat for ICANN s mu t stakeho der mode . Mu t p e r sks assoc ated w th the ncrease n nat ona eg s at on and regu at ons	Cont nue bu d ng understand ng at the nat ona /reg ona /IGO eve about the techn ca way the Internet funct ons, and w th n that what s ICANN s ro e n ma nta n ng a stab e g oba y nteroperab e Internet. Rema n engaged n d scuss ons about Internet governance nc ud ng engagement and educat ona outreach to IGOs and other ent t es, d scuss ng ssues that may touch upon ICANN s m ss on n order to ncrease understand ng and awareness of potent a un ntended negat ve consequences to the nteroperab e s ng e Internet. Mon tor add t ona arenas that are d scuss ng eg s at ve, regu atory, or IGO reso ut ons and expand engagement nto these add t ona governmenta arenas. (Cons dered n Operat ng P an; no change n Strateg c P an)
On Financials: The eve of r sk for ICANN s ong-term fund ng s ncreas ng n the face of changes n the marketp ace, deve opments around the expans on of the gTLD name space, and the onset of a g oba recess on/depress on.	Onset of g oba recess on	Fund ng mode s based so e y on numbers of reg strat ons may not be susta nab e n a recess on (That mpact has not current y mater a zed.)	No add t ona act on bes des the dec s on that was a ready made n May 2020 to de ay FY21 Operat ng n t at ves requ r ng ncrementa resources to FY22. Cont nue to mon tor c ose y and reassess the r sk regu ar y. (No changes to strateg c or operat ng p ans)

2020 Trend Proposal	Shift in trend	Impacts on ICANN	Conclusion & Actions Taken
On Unique Identifier Systems: The rap d evo ut on of emerg ng dent f er techno og es requ res ICANN to be respons ve to these changes and ensure that the un que dent f er systems evo ve and cont nue to serve the g oba Internet user base.	No notab e sh fts, ast year s trends rema n true	No new mpacts	No changes to strateg c or operat ng p ans

2 Process & Methodology

As a first step in the strategic planning process, the community, ICANN Board, and ICANN organization (ICANN org) participate each year in strategic outlook trend identification sessions to discuss emerging trends that could affect ICANN. The trend identification process repeats annually to help inform ICANN's strategy in an ever-changing environment.



The ICANN Bylaws (Section 22.5) mandate ICANN to develop a five-year strategic plan, a five-year operating plan, and an annual operating plan. Every year, new trends or shifts in existing trends related to the operating plans (five-year or annual), the budget, or both are factored into the annual iteration of those plans, as appropriate.

2.1 Description of the Trends Identification Sessions

Trend identification session participants from Board, ICANN org, and the community are divided into subgroups and engaged in a brainstorming exercise to identify and track the evolution of trends that may affect ICANN; and evaluate the impacts that these trends pose to ICANN, either in terms of threats or in terms of opportunities. Subgroups share their ideas with the larger group, and additional discussions follow. At the end of the

session, each participant is invited to vote for top three priorities that ICANN should be focusing on.

This year, the sessions were structured around the five areas of focus of ICANN's strategic plan for fiscal years 2021 to 2025:

- **Security** – Relating to cybersecurity, Internet of Things (IoT) vulnerabilities, Domain Name System (DNS) security, root service reliability, resilience, interoperability, and DNS abuse.
- **ICANN's Governance** – Referring to ICANN's governance rather than Internet governance in general, ICANN's multistakeholder model of governance, efficiency and effectiveness, transparency and accountability, inclusiveness, and openness.
- **Unique Identifier Systems** – Evolution of the unique identifier systems in the context of the development of their uses and their user base, considering external technology advancement (such as blockchain, IoT, rise of artificial intelligence, etc.), alternate roots, alternative infrastructures, Universal Acceptance, and Internationalized Domain Names (IDNs).
- **Geopolitics** – Including the effects of legislation and regulation on ICANN, as well as other globalization topics such as the global reliance on the Internet, or Internet fragmentation.
- **Financials** – Including financial sustainability, financial responsiveness to changing industry economics, funding strategies, and cost management.

For ICANN org staff sessions only, a sixth focus area dedicated to organization-specific, internal trends was contemplated this year for the first time:

- **Org's Operational Excellence** – ICANN org internal processes and policies, systems, resources, performance, collaboration, and customer relationship management. [**Note**: these results are reported separately in Appendix C].

Each session was initiated by reviewing previous year's trends with participants and then asking them to questions around the relevance of last year's trend, any notable shifts, or new trends to consider as well as the impacts, opportunities, and priorities arising from those trends.

2.2 Trend Identification Sessions & Data Computation

TREND IDENTIFICATION SESSIONS

Between November 2019 and March 2020, 398 participants (80% staff, 20% community) participated in 21 trend identification sessions collecting 1853 data elements (868 more data elements than the 985 total data elements collected in 2019).

The COVID-19 pandemic brought new challenges to conducting in-person trend identification sessions. While most of the ICANN org sessions were held prior to the pandemic, community sessions scheduled for ICANN67 needed to be rescheduled to virtual forums. Virtual sessions leveraged online tools to enable participants to collectively identify trends in a remote setting.

DATA COMPUTATION

Following each session, results were summarized and shared those participants to gather final feedback before assimilating all results for further analysis. Inputs were also catalogued in a central repository against several criteria:

- **Focus area** of the data element: *Financials* (and domain name industry trends), *Geopolitics*, *ICANN's Governance*, *Operational Excellence*, *Security*, or *Unique Identifier Systems*.
- **Data qualification**: Data points were qualified as a trend, a risk, or an opportunity.
- **Number of votes** received: During each session, participants were asked to vote for what they thought ICANN should consider to be top priorities.
- **Topic**: The core issue primarily discussed in the statement. Our catalog currently contains about 40 topics. Each year, new topics are introduced based on the inputs received, while some previous topics are no longer relevant.
- **Overarching trend** connected to the data element. Overarching trends are identified through consolidation and summarization of similar or related trend statements. Each year, overarching trends are added, removed, or revised to reflect the evolutions observed.

In some cases, the previous year's overarching trend was no longer applicable and was retired; in other cases, data indicated a new overarching trend was needed to reflect an emerging trend.

2.3 Trend Analysis

To analyze the trends, ICANN org formed a liaison network bringing together different subject matter experts from across the organization. For each focus area, the liaisons assessed trends, risks, and opportunities identified through the trend sessions and shared their observations. This analysis is appended to this paper.

2.4 Trend Impact Assessment Approach

The trend impact assessment process connects trends to ICANN's planning efforts by developing recommendations to inform potential adjustments to planned activities over both the short and long term.

The following methodology was followed to conduct the assessment:

1. Identification of **notable shifts** in trends or new trends and their **impacts on ICANN**

2. Determination of the **materiality** and the **immediacy** of the impacts of the trends identified
3. Rationalization of the decisions to update the plans or other decisions using a **materiality/immediacy decision matrix**
4. Decision of strategic or tactical opportunities

2.5 Conclusion and actions taken

Once approved by the ICANN Board, findings on trends and their impacts on ICANN, as well as opportunities they represent and resulting proposed planned activities, were documented in the next ICANN Operating Plan that will be posted for Public Comment in December of this year.

3 Summary of Findings, and Recommendations

With new five-year plans that just came into effect in July of this year, little to no changes were expected to ICANN plans at this time. The assessment made of this year's strategic outlook trends focused on evaluating potential short- and/or long-term impacts of the coronavirus pandemic on ICANN's plans. On the basis of the work to-date, some adjustments to the Operating Plan have been identified as a result of the pandemic in the way the objectives are addressed (timing as an example), but the pandemic itself does not change the strategic objectives of the organization at the five year horizon.

The following list of trends is the result of the 2020 trend identification sessions and trend assessment that is documented in Appendix B. The trend numbers (e.g., [2.2]) reference previous years' trends and allow tracking of how trends evolve over the years. Organizational Excellence trends can be found in Appendix C.

Trends indicated 'top priority'—those that emerged through statistical analysis and were elevated by the Network Liaison team—are further elaborated in this section in terms of impacts on ICANN and recommendations.

Focus Areas	2020 Trends Proposals	Top Priority
Security	[2.2] DNS ecosystem security threats remain high and have the potential to erode the public trust in ICANN's ability to fulfill its mission.	X
Security	[1.15] There is increasing pressure from the community for ICANN to address "DNS abuse" issues; however, questions remain – with no clear consensus –	X

Focus Areas	2020 Trends Proposals	Top Priority
	about what constitutes “DNS abuse", and about what ICANN’s role should be in relation to “DNS abuse".	
Unique Identifier Systems	[1.07] The rapid evolution of emerging identifier technologies requires ICANN to be responsive to these changes and ensure that the unique identifier systems evolve and continue to serve the global Internet user base.	X
	[1.13] The increasing use of internationalized and generic domain names is an opportunity for ICANN to be proactive about universal acceptance, as appropriate within its mission.	
Geopolitics	[3.7] There is an increased effort by national and regional governments as well as intergovernmental organizations and other types of initiatives to regulate or legislate the Internet. This trend has the potential to lead to actions threatening the operability and openness of the Internet and increases the complexity of ICANN operations and policy development.	X
Governance	[3.1] COVID-19 pandemic-related disruption is accelerating community's interest to evolve ICANN’s multistakeholder model to be agile in the face of change and to support equitable, efficient processes for effective decision-making.	X
	[1.01] There is a continued necessity to fulfill transparency, accountability, inclusiveness, and openness obligations.	
	[1.03] There is increasing community awareness about the Empowered Community’s powers and responsibilities and how those are exercised.	
	[1.04] Heightened public awareness of ICANN, coupled with a lack of understanding about its role, threatens legitimacy and public trust in ICANN and increases the need to communicate broadly on ICANN's role. The ease of spreading misinformation through social media, traditional media and other channels further impacts clarity about ICANN's role.	
	[1.10] As community discussions become more complex and technical, there is increasing demand from non technical stakeholders to better understand technical topics. At the same time, uncertainty is growing among technical stakeholders about where and how to make their voices heard.	
Financials	[1.02]: The level of risk for ICANN’s long-term funding is increasing in the face of changes in the marketplace, developments around the expansion of the gTLD name space, and the onset of a global recession/depression.	X
	[1.14]: Prioritization is becoming more critical, to continue to support the growing needs and demands of ICANN’s global community	

More trend assessment details including trend elements, risks, opportunities, and observations from network liaisons are provided in Appendix B. Trends regarding Organizational Excellence are provided in Appendix C, since these pertain internally to the organization. The remainder of this section outlines top-priority trends, notable shifts, impacts, and resulting recommendations across each of the five focus areas.

3.1 Security Findings and Recommendations

On security, the Strategic Outlook process led to the following main conclusions:

- Priority Trend #2.2: DNS ecosystem security threats remain high and have the potential to erode the public trust in ICANN's ability to fulfill its mission.
    - *Notable shifts*: Increased reputational risk inherent to the lack of understanding of ICANN's role.
    - *Main Impacts*: Continued heightened security threats are eroding public perception about the integrity of the system, potentially hampering ICANN's ability to fulfill its mission.
    - *Recommendations*: Opportunity to align perceptions and draw a distinction between DNS ecosystem security threats and DNS Abuse; to create awareness of the differences between the two and magnitude of each; and to explain ICANN's role in addressing DNS security threats. (Considered in Operating Plan; no change in Strategic Plan)

- Priority Trend #1.15: There is increasing pressure from the community for ICANN to address "DNS abuse" issues; however, questions remain – with no clear consensus – about what constitutes "DNS abuse", and about what ICANN's role should be in relation to "DNS abuse".
    - *Notable shifts*: n/a (new trend)
    - *Main Impacts*: Increases in "DNS abuse" are affecting user security, having an impact on ICANN's credibility, and making the Internet untrustworthy.
    - *Recommendations*: Opportunity for community to align on what constitutes DNS abuse and what ICANN's role should be in combating abusive use of the DNS (Considered in Operating Plan; no change in Strategic Plan)

3.2 Unique Identifier Systems Findings and Recommendations

On Unique Identifier Systems, the Strategic Outlook process led to the following main conclusions:

- Priority Trend #1.07: The rapid evolution of emerging identifier technologies requires ICANN to be responsive to these changes and ensure that the unique identifier systems evolve and continue to serve the global Internet user base.

- *Notable shifts*: No notable shifts, last year's trends remain true.
- *Main Impacts*: No new impacts.
- *Recommendations*: No changes.

3.3 Geopolitics Findings and Recommendations

On Geopolitics, the Strategic Outlook process led to the following main conclusions:

- Priority Trend #3.7: There is an increased effort by national and regional governments as well as intergovernmental organizations and other types of initiatives to regulate or legislate the Internet. This trend has the potential to lead to actions threatening the operability and openness of the Internet and increases the complexity of ICANN operations and policy development.
  - *Notable shifts*: The COVID-19 pandemic has moved more spheres of life online.
  - *Main Impacts*: The COVID-19 pandemic increases the risk of governmental interventions due to the increased perception of Internet and Internet-based services as essential utilities. The push to a multilateral model of Internet governance is an existential threat for ICANN's multistakeholder model. Multiple risks associated with the increase in national legislation and regulations
  - *Recommendations*:
    - Continue building understanding at the national/regional/IGO level about the technical way the Internet functions, and within that what is ICANN's role in maintaining a stable globally interoperable Internet.
    - Remain engaged in discussions about Internet governance including engagement and educational outreach to IGOs and other entities, discussing issues that may touch upon ICANN's mission in order to increase understanding and awareness of potential unintended negative consequences to the interoperable single Internet.
    - Monitor additional arenas that are discussing legislative, regulatory, or IGO resolutions and expand engagement into these additional governmental arenas.

      This is needed, as the global pandemic has moved more spheres of life online, which has further raised the profile of the Internet and its possible vulnerabilities to the attention of governments, often requiring actions from aspects of these governments that had not

participated in the multistakeholder model in the past.
(Considered in Operating Plan; no change in Strategic Plan)

3.4 ICANN's Governance Findings and Recommendations

On ICANN's Governance, the Strategic Outlook process led to the following main conclusions:

- Priority Trend #3.1: The COVID-19 pandemic-related disruption is accelerating community's interest to evolve ICANN's multistakeholder model to be agile in the face of change and to support equitable, efficient processes for effective decision-making.
    - *Notable shifts*: Community participation concerns exacerbated by prolonged virtual settings (inability to meet face-to-face)
    - *Main Impacts*: Reduced or insufficient community participation could slow down community's work and risks capture and threat to ICANN's multistakeholder model due to loss of trust, credibility, and legitimacy.
    - *Recommendations*: Opportunity to evolve both the ICANN public meetings strategy and the planning and implementation of the work on Enhancing the Effectiveness of ICANN's Multistakeholder Model
      (Considered in Operating Plan; no change in Strategic Plan)

3.5 Financials (and Domain Name Industry) Findings and Recommendations

On Financials, the Strategic Outlook process led to the following main conclusions:

- Priority Trend #1.02: The level of risk for ICANN's long-term funding is increasing in the face of changes in the marketplace, developments around the expansion of the gTLD name space, and the onset of a global recession/depression.
    - *Notable shifts*: Onset of global recession
    - *Main Impacts*: Funding models based solely on numbers of registrations may not be sustainable in a recession (That impact has not currently materialized.)
    - *Recommendations*: No additional action besides the decision that was already made in May 2020 to delay FY21 Operating initiatives requiring incremental resources to FY22. Continue to monitor closely and reassess the risk regularly. (No changes to plans)

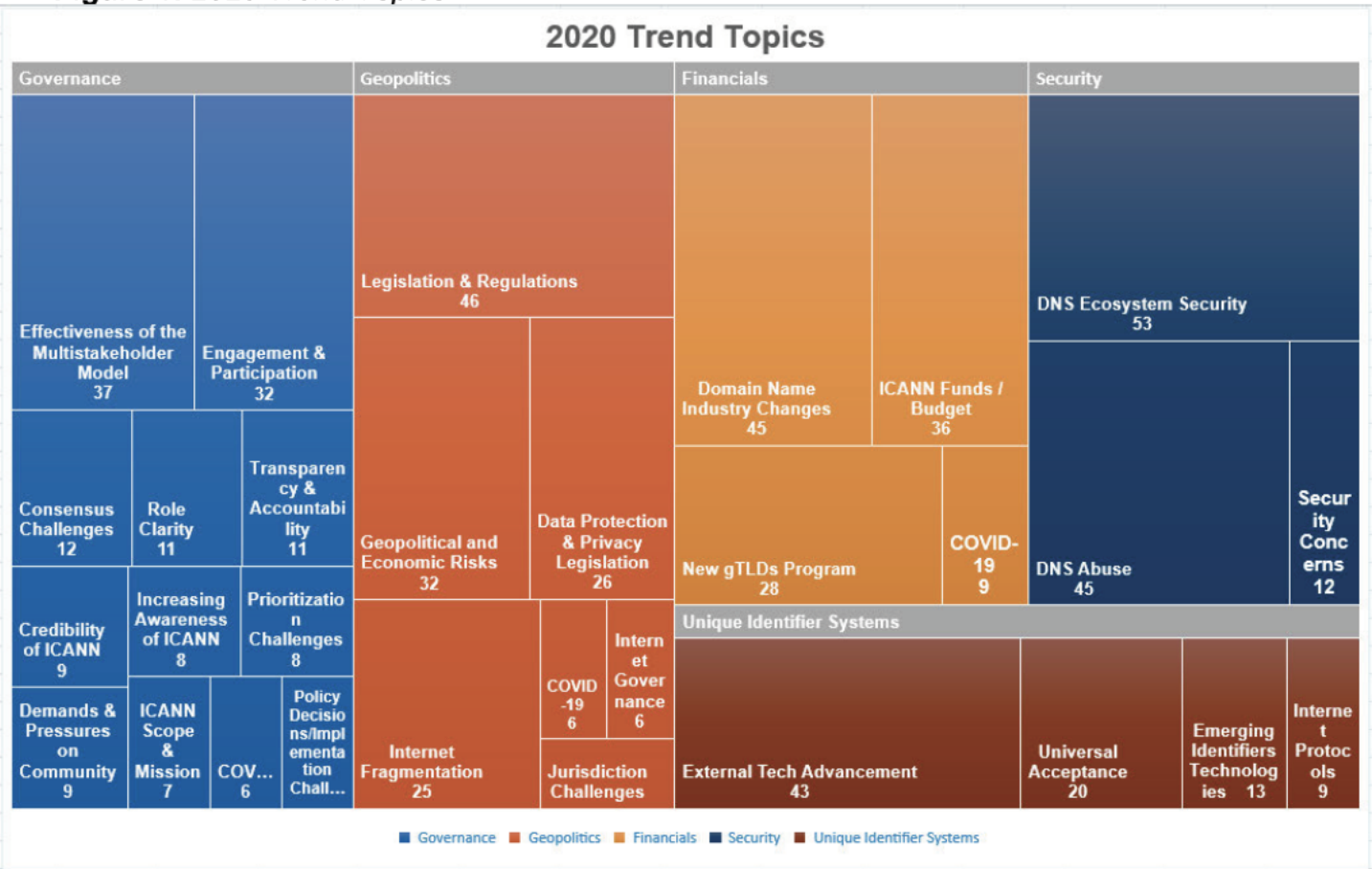
4 Appendices

Appendix A | Statistical Analysis

2020 Trend Topics

The 2020 Trend Topics chart (**Figure 1**) provides an analysis of the inputs that reflects the level of attention these topics received in 2020. Topics are first organized by focus area (e.g., Governance) and then by topic (e.g., Engagement & Participation).

Figure 1. *2020 Trend Topics*



Note: *Due to space limitations in the above chart for the smallest rectangles two topic names are incomplete as denoted by the ellipsis in the bottom right corners of both the Governance focus area. These should read "COVID-19" and "Policy Decisions/Implementation Challenges". Each of these topics had six statements associated with it for 2020.*

In 2020, the focus areas of ***Governance*** and ***Geopolitics*** received the greatest volume of comments, followed by *Financials, Security, and Unique Identifier Systems.*

To illustrate how the top 20 trend topics of 2020 compare to 2019, **Figure 2** below shows a comparison ranked by number of votes per topic. The *Number of Statements* column indicates the number of data points related to that topic in a given year (e.g., popular or hot topics). *DNS Ecosystem Security*, *Effectiveness of the Multistakeholder Model,* and *External Tech Advancement* are the hot topics for 2020. The *Tiered* column percentages indicate that topic's number of votes as compared to the top-voted topic (which is shown as 100%). This provides a visualization of which topics were in the top, middle, and bottom tiers in terms of number of votes.

The chart uses a heat map in the final column of the chart to compare the ranked position of the top 20 trend topics in 2020 to the ranked position of the same topics in 2019. This heat map shows which topics had the greatest movement between these two years. The green fields highlight which topics saw the greatest increase in emphasis and the red fields show the topics that have fallen in importance.

***Figure 2**. Top 20 Topics in 2020 in Comparison to 2019*

2020 Top-20 Topics	# of Statements	# of Votes	Tiered	2020 position	2019 position	Heat Map
DNS Ecosystem Security	54	41	79%	1	12	11
Effectiveness of the Multistakeholder Model	37	36	69%	2	2	0
External Tech Advancement	48	35	67%	3	4	1
DNS Abuse	47	28	54%	4	35	31
Universal Acceptance	20	23	44%	5	26	21
ICANN Funds / Budget	37	22	42%	6	17	11
New gTLDs Program	29	21	40%	7	25	18
Engagement & Participation	32	19	37%	8	31	23
Data Protection & Privacy Legislation	28	18	35%	9	8	-1
Role Clarity	18	18	35%	10	43	33
Legislation & Regulations	48	17	33%	11	1	-10
Credibility of ICANN	9	17	33%	12	--	new
Consensus Challenges	12	17	33%	13	28	15
Geopolitical and Economic Risks	37	16	31%	14	13	-1
ICANN Scope & Mission	10	14	27%	15	40	25
Domain Name Industry Changes	50	14	27%	16	15	-1
Risk of Capture	4	12	23%	17	--	new
Security Concerns	12	12	23%	18	21	3
COVID-19	26	11	21%	19	--	new
Internet Fragmentation	29	11	21%	20	9	-11

Top tier (67%-100%) **2nd tier** (34%-66%) **3rd tier** (0%-33%)

In 2020, *DNS Abuse, Role Clarity,* and *ICANN Scope & Mission* received the highest increase in priority votes year-over-year, while *Legislation and Regulations* and *Internet Fragmentation* showed the greatest drop in emphasis as compared to 2019.

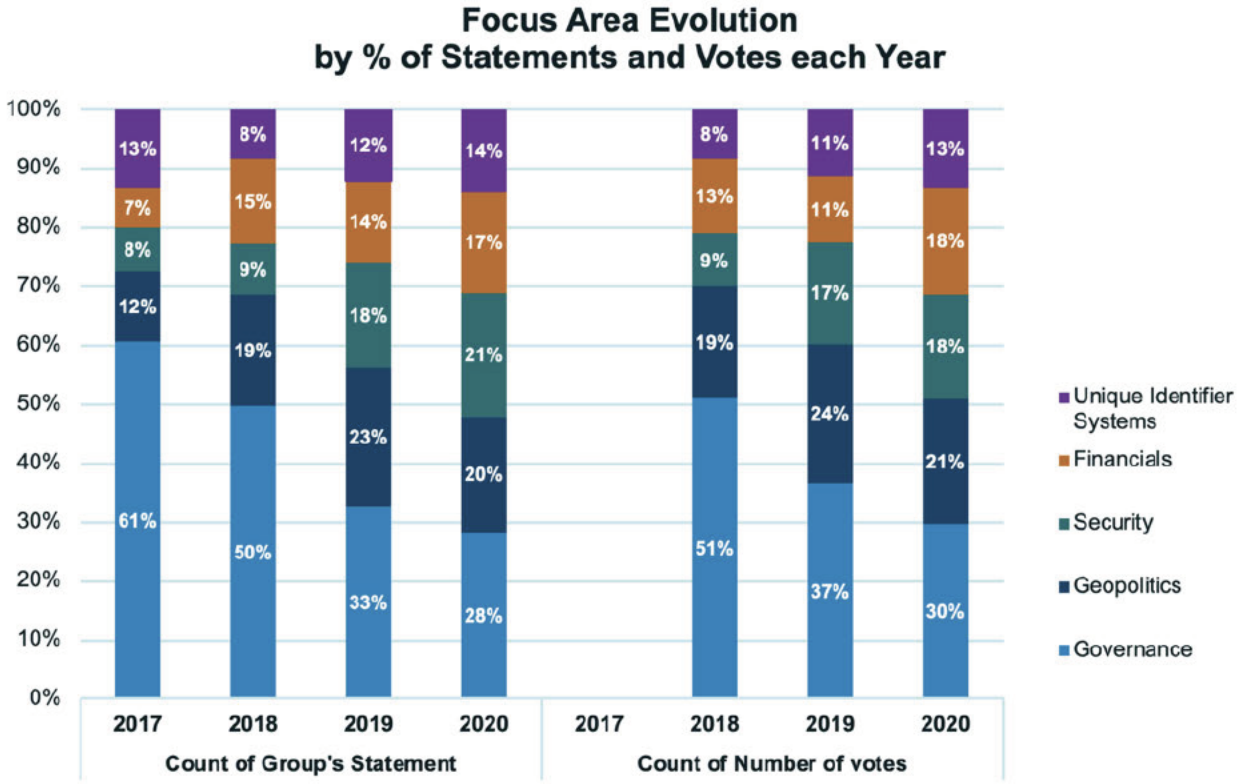
New trend topics introduced in 2020 were:

- Business Continuity
- Career Development
- Complexity of Topics to be Dealt With
- Coordination & collaboration
- COVID-19
- Culture
- Decision Making process / Delegation of Authority
- Emerging Identifiers Technologies
- Inclusiveness
- Internet Protocols
- Root Server Security
- Succession Planning

Evolution of Trend Focus Areas Over Time

Figure 3 below provides an overview of how focus areas have evolved since 2017, based on the number of statements and votes for each focus area. Since 2017, *Governance* has continued to lead all other focus areas in terms of number of statements or votes. However, this margin has been shrinking gradually every year, notably from 61% of all statements in 2017 to 28% of all statements in 2020. The chart illustrates increased emphasis on *Unique Identifier Systems*, *Financials*, *Security*, and *Geopolitics* and a decreased emphasis on *Governance*.

***Figure 3**: Focus Area Evolution*

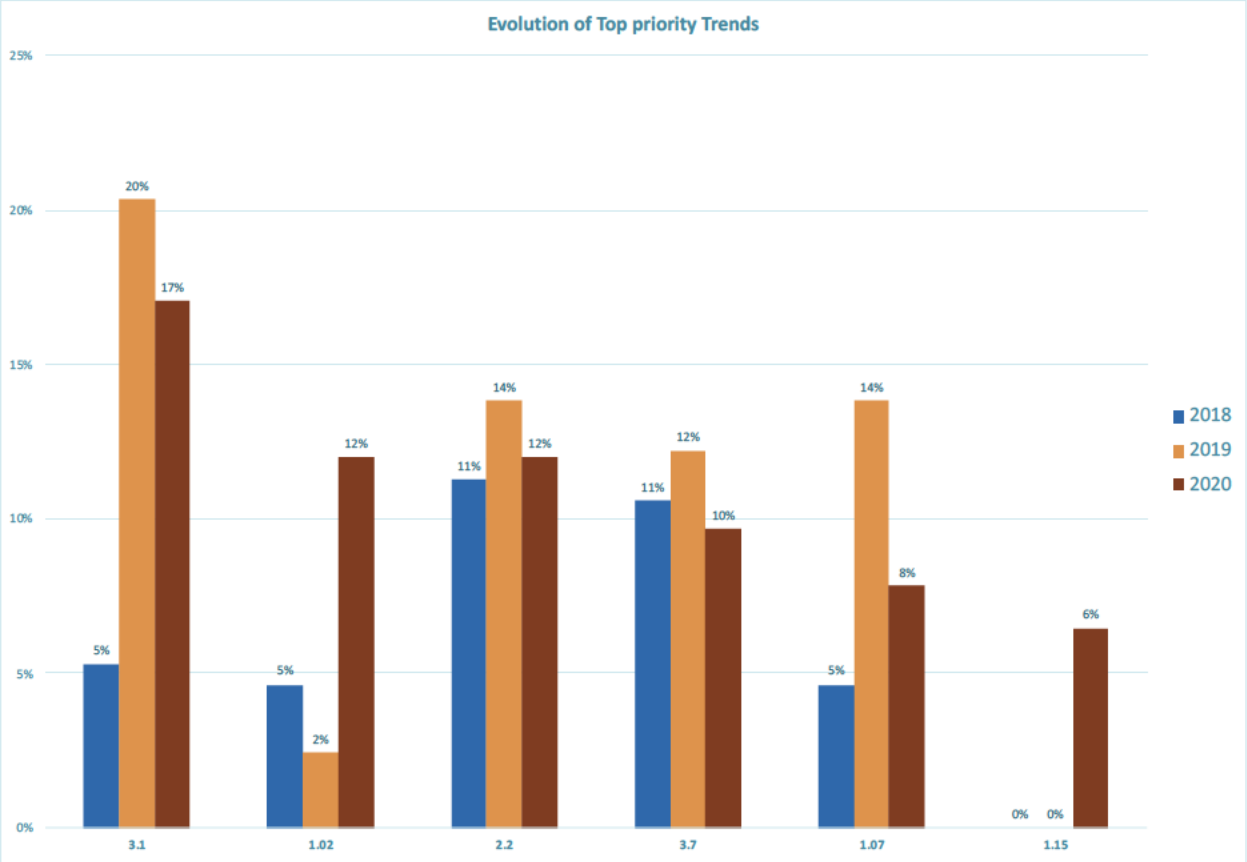


Note: There was no voting in 2017, which is why there is no data for that year.

Evolution of Top Priority Trends Over Time

Figure 4 below illustrates the trends that received the most votes in 2020, compared to their priority (based on vote count) in the previous three years. It is calculated based on the ratio of the number of votes for each trend over the total number of votes for a given year.

***Figure 4**: Evolution of Top Six Priority Trends*



***Note**: Bar graph labels are rounded to the nearest one and do not reflect exact values.*

***Fig. 4 Key:** Evolution of Top Priority Trends (left to right)*	**Noteworthy Evolution**
2.2 (Trend relating to DNS ecosystem security)	Steady annual increase in priority for last 3 years
3.1 (Trend relating to ICANN's multistakeholder model)	Remains top priority
1.02 (Trend relating to Domain Name industry changes & impacts on funding)	Sustained priority over years
2.2 (Trend relating to DNS ecosystem security)	Steady annual increase in priority for last 3 years
3.7 (Trend relating to legislation & regulations)	Sustained priority over years
1.07 (Trend relating to the emerging identifiers technologies)	Sustained priority over years
1.15 (Trend relating to DNS Abuse)	New 2020 trend (no data from previous years)

Appendix B | Focus Area Trend Assessment

Purpose of Document

The purpose of the Trend Assessment is to summarize the results of this year's trend identification sessions, and, where possible, to:

- Provide additional observations noted by the Strategic Outlook Network.[1]
- Identify noticeable shifts in trends or new trends that may be worth highlighting.

This document was prepared by the Multistakeholder Strategy and Strategic Initiatives (MSSI) team in collaboration with the Strategic Outlook Network liaisons. It was intended for the Executive team, the Strategic Planning Board Working Group, and the entire ICANN Board as input into the next step of the strategic planning process.

Please note: One of the roles of the Strategic Outlook Network liaisons was to review trend statements, risks, and opportunities and address significant inaccuracies or areas that required further elaboration to clarify the point. In some cases, these statements represent perceptions from participants in the trends sessions. Inclusion of those statements is intended to reflect the data collected and is **not intended as an endorsement**. In cases where the Strategic Outlook Network had a different opinion or felt that a trend/risk/opportunity statement represented a perception rather than a fact, it is explicitly indicated as such. These instances are elaborated in each Focus Area section titled **Additional Observations from ICANN Org's Strategic Outlook Network.** In some cases, words or phrases are in quotations as a reflection of what was heard in the trend sessions but to clarify that these are not necessarily well defined or agreed upon. For example, the term 'DNS Abuse' was frequently mentioned in the trend sessions but this term has different meaning across various stakeholder groups.

Security Trends

- **Summary of Trend Elements Collected During the Trend Sessions**

  DNS ecosystem security threats remain high. Specific DNS security challenges include:

[1] The Strategic Outlook Network is a cross-functional and cross-regional team of ICANN staff, who act as liaisons for the strategic outlook-related work in their respective function or region. The liaisons provide subject matter expertise and share their observations around key findings in order to provide context and flag any key issues that need to be taken into consideration in the formulation of recommendations.

- Weakened cryptographic algorithms (e.g., SHA-1).
- Combination of 5G (which bypasses most local infrastructure) and Internet of Things (which increases the number of points of vulnerability) constituting a major threat.
- Increase in domain name registrations related to phishing and other fraudulent schemes.
- Increasing use of IDNs for phishing and homograph attacks.
- Widespread ransomware attacks against unpatched systems and organizations.
- Crisis-driven abuse risks (e.g., COVID-19-related abusive domain name registrations and behaviors).

There is an increased pressure from the community for ICANN to address "DNS abuse" issues, but questions remain – with no clear consensus – about what constitutes "DNS abuse," and about what ICANN's role should be in relation to "DNS abuse." Some parts of the community appear to want ICANN to take a more active role that is more than just educational in nature.

Cybersecurity is increasingly becoming a geopolitical matter, not just a technical concern. For example, European governments are strongly engaged in the matter (e.g., digital sovereignty, digital services act), and the United Nations has taken some serious steps in that area, as well. At the same time, challenges to combating DNS abuse remain or increase. Some of the challenges noted include:

- The implementation of data privacy legislation is making it harder to identify potential abusers.
- ccTLDs have no contractual obligations to combat DNS abuse.
- DNSSEC adoption is stagnant with key actors (browser vendors) resistant to further steps (e.g., DANE[2]).

The COVID-19 pandemic is adding more challenges to maintaining the security of the unique identifier systems. The pandemic is making it challenging to access root servers and server systems while also requiring adaptations to the process

[2] DANE: DNS-based Authentication of Named Entities

to run key signing ceremonies. Smaller TLD operators may not have the ability to work remotely during the pandemic, leading to challenges in supporting TLD infrastructure. Cyber-attacks on remote or online participation tools (e.g., *"Zoom bombing*") are likely to increase as more people use these tools. COVID-19 related "DNS abuse" also needs to be considered.

Finally and separately, it was noted that the governance structure of the Root Server System is evolving (through the implementation of SSAC037 & SSAC038).

- **Summary of Risks Identified During the Trend Sessions**
    - Increases in "DNS abuse" and DNS ecosystem security threats are affecting user security, having an impact on ICANN's credibility, and making the Internet untrustworthy.
    - If security threats are not addressed, there are risks of greater government intervention in DNS security-related matters through legislation. This can affect both Internet functionality and interoperability.
    - Continued risk of attacks to ICANN systems could paralyze IANA functions and ICANN org operations.
    - Evolving governance structure of the Root Server System may impact the relationship between ICANN and root server operators (implementation of RSSAC037 & RSSAC038).
- **Summary of Opportunities & Suggested Actions Identified During the Trend Sessions**
    - Reach a shared definition of "DNS abuse" within the ICANN ecosystem in order to collaborate effectively.
    - Increase communication and education of the larger community and public to clarify ICANN's role in relation to "DNS abuse" and to raise awareness of "DNS abuse" information beyond the technical community, thereby helping end users understand how to protect themselves online.
    - Push for more Domain Name System Security Extensions (DNSSEC) adoption with key actors, including: ccTLDs, registrars, registries, resellers, Internet service providers (ISPs), network operators, vendors, etc.

- To reduce Internet of Things (IoT) vulnerabilities, increase awareness about endpoint hygiene and IoT's impact on the DNS.

- **Additional Observations from ICANN Org's Strategic Outlook Network**

  DNS ecosystem security threats cover a broad range of issues, and not all of them are within ICANN's mission. ICANN has a role in mitigating some of these threats and abuses, some others ICANN can influence, and others are out of ICANN's reach. Currently, there is no collective agreement across the ICANN community of what "DNS abuse" encompasses. Several community groups are engaged in discussions about "DNS abuse," but there is no coordinated effort across all the community groups yet. The plenary sessions at recent ICANN Public Meetings have served as a mechanism for cross-community updates and discussions but have not as yet resulted in agreed concrete actions for the community as a whole. It is also unclear if any additional concerted community action is necessary, over and above what some groups (including ICANN org) are already doing.

  The increased awareness of DNS security issues accompanied by a vast incomprehension of ICANN's role creates a reputational risk for ICANN. While there does not appear to be a demand for ICANN to broaden its mission at this point, there seems to be a need to increase the public awareness of what ICANN's role is and what ICANN does to mitigate DNS ecosystem security threats.

  On the geopolitical front, ICANN's continuous outreach effort towards the United Nations (UN) and the UN General Assembly committees has resulted in better understanding among the diplomats about ICANN's mission. This is very useful in deliberations that touch on the security, stability, and resiliency of the Internet and the DNS. During some of the discussions at the UN, different member states have mentioned what ICANN does, without naming the organization, as areas, which should be at the least discussed by the UN. ISOC has sent comments to the Open-ended Working Group (OEWG), where they state, "The Internet's public core encapsulates the Internet routing, naming and numbering systems (the Domain Name System), security and identity cryptography mechanisms." The ITU World Telecommunications Standardization Assembly (WTSA), the ITU Council Working Group on international Internet-related public policy issues, as well as other WGs have also been discussing ICANN-related issues, including gTLDs and new Internet Protocols ("new IP").

Some participants cited “weaponization” of the Internet as a trend without providing an underlying explanation. While cyberattacks and other offensive acts by companies (e.g., industrial espionage) and by individuals (e.g., ransomware) continue, attacks by state actors and organized criminal groups appear to be increasing.

Other initiatives underway by ICANN org include:

- The Domain Abuse Activity Reporting (DAAR) provides encouragement and useful information for TLDs to combat DNS abuse.
- The DNS Security Facilitation Initiative (DSFI) was introduced in May 2020, to investigate mechanisms to strengthen collaboration and communication on security and stability issues.

Unique Identifier Systems Trends

- **Summary of Trend Elements collected during the Trend Sessions**

  Encrypted DNS protocols, such as DNS over HTTPS (DoH) and DNS over TLS (DoT) represent a major evolution of the DNS, and associated deployment models may change the way DNS is handled.

  Increased introduction of alternative technologies and attempts to bring new identifier systems to life, some of them being advertised as a “replacement for the DNS.” Specific examples include:

  - Huawei is advocating for a new set of Internet protocols dubbed “new IP” (Internet Protocol) in the ITU Telecommunication Standardization Sector (ITU-T) and other standards development organizations, claiming that the current TCP/IP protocol suite is not capable of handling new challenges facing the Internet, such as significantly higher bandwidth consumption, the need for deterministic (predictable) network performance, and new security requirements.
  - Alternate root systems based on blockchain technology (e.g., Ethereum Name Service, etc.) create increasing confusion and instability.
  - National pushes for autonomous identifier systems (e.g. Russia’s recent "sovereign Internet law" exercise, China’s “Great Firewall”).
  - The use of keywords in browsers, proprietary social networks, or the use of apps on mobile devices, etc., could render generic domain names obsolete.

  Usage of IDNs is increasing in APAC, and there is potential for greater adoption of Universal Acceptance within the next two years. However, software and email providers and IT infrastructures are not becoming UA-ready largely due to lack of understanding or lack of capacity.

  IPv6 deployment continues to be limited. IPv4 depletion and increased pricing of IPv4 space is causing headaches for providers and leading to abuse and “gaming”. Somewhat related, there seems to be a larger trend around service readiness, and pushing new technology that, at times, ICANN and/or its vendors are not ready for (e.g., IPv6, IDNs and other UA issues).

The unexpected growth of global Resource Public Key Infrastructure (RPKI) adoption in 2019 leads to interesting questions about its scalability and viability. RPKI can introduce complexities which could impact network complexities. As more networks secure their routing, challenges may arise, as well as the question of ICANN's role.

Besides the well-known (global) public DNS servers (e.g., Google, Cloudflare), there is a noted higher demand for DNS public services, particularly from regional operators (e.g., Tencent).

- **Summary of Risks Identified During the Trend Sessions**
    - Risks of (more) centralization of resolvers, and possibly fragmented Internet namespace due to DoH/DoT deployment models.
    - Potential alternative Root Server Systems and increased interest in emerging technologies such as IoT or blockchain are increasing the risk of Internet fragmentation and calling into question ICANN's relevance in the future as traditional identifiers may become irrelevant.
    - Having the RPKI trust anchor returned to IANA would involve significant risk (similar to managing the root zone key signing key).
    - It is unclear if ICANN is able to meet the evolving needs of the world if it has many people (among staff and community) that do not know enough about technology or are resistant to change.
- **Additional Observations from ICANN Org's Strategic Outlook Network**
    - DoT and DoH introduce local policy implications on encrypting DNS traffic, increasing the complexity of monitoring and filtering DNS traffic while changing communication privacy. They have the potential to move the control point for DNS policy from ISPs to web browsers.
    - Proprietary social networks, mobile apps, etc., are still utilizing and relying on standardized unique identifiers. As such, they do not put at risk the unique identifier systems.
    - There appears to be a growing appetite from the community for more technical discussions and more capacity building on technical topics. It could be interesting to survey the community to get a better understanding of where the gaps are with what is currently being provided through

ICANN Public Meetings ”Tech Day” sessions, and other existing technical engagements efforts.

Geopolitics Trends

- **Summary of Trend Elements Collected During the Trend Sessions**

  Putting at risk the singularity and openness of the Internet, the global trend of protectionism continues, materialized by :

  - National and regional government legislations and regulations (California Consumer Privacy Act, Chinese data protection law, Russia Sovereign Internet law, etc.)
  - Localized content controls or blackouts.
  - Control of Internet access.
  - Country sanctions (e.g., tariffs).
  - Regulation of data flows across country borders.

  The implementation of local legislations and regulations (e.g., ePrivacy Directive, General Data Protection Regulation) continue to encroach on the Internet and ICANN's operations. Unintended consequences of legislation and regulations negatively impact the DNS and its infrastructure:

  - Poorly designed or worded legislation threatens the ability of the Internet to operate the way users expect it to (fast and well).
  - Data privacy legislation is hindering ICANN and other actors' ability to mitigate DNS abuse.
  - New emerging privacy laws may also not all converge on one standard of protection.
  - More requests for ICANN to assist law enforcement agencies, increasing ICANN's workload (due to unavailability of public WHOIS data).

  Pandemic-related pressure may cause some states to revisit their national and state privacy legislations and relax privacy considerations under the guise of monitoring for public health reasons, which may be perceived as an overstep. It is also possible government bodies may reconsider the societal and economic

importance of Internet infrastructure in terms of enacting new protectionist measures.

The question of ICANN's jurisdiction continues to be a subject of discussions, as well as the broader topic of cross-border legal challenges facing the Internet. The recent intervention by the California Attorney General in the .ORG/Public Interest Registry change of control request has revived the conversation (at least in mailing lists) in the community about ICANN's jurisdiction. It raises a question about ICANN's independence from the U.S. government and could initiate renewed conversation as to whether ICANN's jurisdiction should change.

Outside of discussions regarding ICANN's jurisdiction, the Secretariat of the Internet & Jurisdiction Policy Network launched the world's first Internet & Jurisdiction Global Status Report at the United Nations Internet Governance Forum on 27 November 2019. It presents a first-of-its-kind mapping of Internet jurisdiction-related policy trends, actors, and initiatives.

There has been an increased media attention on ICANN due to recent events (e.g., COVID-related DNS abuse) and decisions (e.g., delegation of .AMAZON decision, Public Interest Registry change of control request, .COM contract renegotiation with Verisign), accompanied by a growing public misperception of ICANN as a political or regulatory body instead of a technical organization.

There is an increased interest in all things cyber (security, crime, Internet governance, data sovereignty, etc.) among intergovernmental organizations (IGOs), especially within the United Nations. Discussions about Internet norms are increasing (e.g., IGF, UN, other initiatives – Microsoft, Paris Call for Trust and Security in Cyberspace). Several initiatives related to Internet governance are putting pressure on the multistakeholder model:

- UN-related proposals for new intergovernmental Internet-related bodies.
- Other IGOs like the ITU, where member states might bring agenda items which fall under ICANN's mission to upcoming conferences (as they have done in the past).
- Proposal to establish a new high-level UN technology envoy position.
- Suggested changes in the Internet Governance Forum (IGF).
- Some UN member states are publicly complaining that the current model of DNS/IP address allocation is not fair.

- Increase in using government agencies to investigate or influence ICANN or its transactions.

At the ITU, certain member states are trying to push different technological proposals, some of which are aimed at the unique identifiers. At least one technological proposal suggests that a new Internet Protocol is needed for the 5G world.

ICANN's level of engagement in global Internet governance (IG) forums (limited sponsoring and contribution to IG schools, national and regional IGFs) may have been perceived by some in the community and organization as a sign of ICANN's disengagement from that space.

The multilateral pressure on ICANN's multistakeholder model increases. There is new pressure from outside ICANN to replace or diminish ICANN's role in favor of multilateral, intergovernmental organizations and alliances. More countries are talking about "digital sovereignty" and the "unfair model" of DNS/IP address allocation. Governments will continue to be pressed to act or intervene where Internet problems are identified, like privacy, security, and questionable content. For instance, some countries are using "mandated by IGO" as cover for implementing restrictive national regulatory policies. There are proposals for a new Internet Protocol (new IP), suggested at the ITU.

The COVID-19 pandemic has brought increased focus on the importance of the Internet, including by governments on ICANN's role in coordinating the Internet's unique identifiers.

- **Summary of Risks Identified During the Trend Sessions**
  - Loss of trust in ICANN's multistakeholder model and potentially Internet governance more broadly could result in more national legislation or other forms of government and IGOs interventions or calls for different multilateral forms of Internet governance. The push to a multilateral model of Internet governance is an existential threat for ICANN's multistakeholder model.
  - Multiple risks associated with the increase in national legislation and regulations:
    - Privacy laws could yield an increase in DNS abuse.

        - Challenges for ICANN to keep pace with new legislations, and reputational and financial risks if ICANN breaches regulations.
        - More legal challenges and conflicts with ICANN policies. Increased complexity to develop policies.
    - Risk of increased Internet fragmentation, jeopardizing the interoperability of the Internet.
    - The COVID-19 pandemic increases the risk of governmental interventions due to the increased perception of Internet and Internet-based services as essential utilities.

- **Additional Observations from ICANN Org's Strategic Outlook Network**

  The trend of national legislations calling for the creation of "sovereign DNS", poses a threat to the uniform development and use of the unique identifier systems, which can disrupt a single stable globally interoperable Internet.

  It is important to note that new national or regional regulations or other forms of governmental interventions in DNS-related matters might take place, even if there is no loss of trust in ICANN. These could be also motivated by a desire for more control on the national level, which some governments say the multistakeholder model does not give them.

  There appears to be a lack of knowledge or awareness among both staff and community of what ICANN already does in terms of monitoring of legislation initiatives, government engagement, and relating to Internet governance. The reporting effort on emerging legislations and regulations initiated by ICANN org in 2018 had to be temporarily placed on hold for various reasons. ICANN org needs to do a narrative report to clarify where things stand. Recent changes of approach by the Government Engagement team may need to be communicated with all staff.

  Broader community's lack of understanding of ICANN's role as a technical organization can be addressed via additional outreach and engagement efforts, aiming at clarifying ICANN's role.

ICANN's Governance Trends

- **Summary of Trend Elements Collected During the Trend Sessions**

  ICANN's multistakeholder model continues to face effectiveness and efficiency challenges. Evolution of the community work is apparent. Examples of the evolution include the Board members participating directly with working groups as liaisons, and in the efforts to coordinate and collaborate between SOs and ACs through the SO/AC leaders' meetings. Some questions were raised regarding the effectiveness of the process initiated to evolve the model, and possible overlaps between different initiatives under way.

  Numerous more specific concerns were raised relating to community participation.

  First and foremost, ICANN's ability to ensure community participation and newcomer retention is questioned. Associated concerns about volunteer burnout among stakeholders trying to keep up with policy responsibilities continue to be voiced. There is not enough generational shift in participation – something necessary for the multistakeholder model to work effectively in the future.

  It can be challenging to ensure participation of both technical and nontechnical stakeholders in ICANN's complex discussions. While there is increased interest among nontechnical stakeholders to learn and more effectively engage, many still lack knowledge of where and how to best do so. In addition, some technically inclined stakeholders are seeking opportunities to engage in more complex technical discussions, beyond the educational ones currently available (e.g., Tech Day & the DNSSEC and Security Workshop; evolution of the Technical Experts Group into the Special Interest Forum on Identifiers Technology, known as SIFT).

  Several external factors, such as carbon footprint, climate change, and global health risks, are also putting pressure on ICANN's model of participation. The current shift to remote-only participation caused by the COVID-19 pandemic raises concerns for participation. It is important to recognize that a majority of new Internet users are non-English speakers and that many stakeholders do not have affordable or reliable Internet access to participate in remote sessions. With the pandemic eliminating face-to-face meetings, ensuring diverse participation while maintaining productivity will become difficult.

  The need for diversity, balance, inclusivity, and openness continues to be reaffirmed, but many challenges remain, to ensure all relevant interested stakeholders are included to ensure diverse and balanced representation in the

community. Structural silos in the governance model need to be overcome. Desire for diverse participation is also sometimes perceived to be at odds with efficient consensus-based decision-making.

Reaching agreement in policymaking processes is becoming more challenging as participants show less willingness or ability to move beyond their self-interests in order to compromise or collaborate. There is also some tension around the degree to which expert vs. non-expert opinions are given equal consideration in a decision-making process. These trends make it more difficult to reach consensus and to be agile in response to changing conditions (e.g., new regulatory requirements such as GDPR).

The community is still adjusting to the new bylaws. There are some misunderstandings of the scope and powers of the Empowered Community, such as calls to refer items to the Empowered Community that are outside of its mandate. There is also confusion as to the scope of some of the Empowered Community powers. For example, in FY2020 we saw a first attempt to use the Inspection Right that sought information beyond the Bylaws' limitation of books and records. While no formal challenges were raised to ICANN's denial of the out of scope request, ICANN critics have pointed to that denial as an example of ICANN's lack of accountability to its Empowered Community. We expect the trend of a need to adjust to and understand the Empowered Community to continue.

Policy work is getting more complex (e.g., the GNSO's New gTLD Subsequent Procedures policy development process (PDP), associated dependencies, coordination with the technical initiative on name collision, and Competition, Consumer Trust, and Consumer Choice Review recommendations implementation). A number of parallel work streams are sometimes seen as uncoordinated or duplicative efforts. For example, there can be concerns about whether the scope of a review team's mandate or its recommendations may raise policy-related questions and implications, and at what stage and how to deal with these issues, including how to invoke the appropriate policy development processes. With regard to reviews, many recommendations are not yet implemented and there is little pause between review cycles, leading to decreased morale and productivity.

Accountability and transparency may be challenged in instances where stakeholders perceive ICANN org to take top-down approaches, such as the pause in implementation of the Privacy and Proxy Services Accreditation policy

and the implementation of the Thick WHOIS policy, as a consequence of the community's policy work related to gTLD registration data.

Recent media and public attention on ICANN, such as with the .AMAZON registry agreement (RA), .COM RA amendment, and the Public Interest Registry change of control request, has spurred misconceptions and differing opinions about ICANN's role in Internet governance. Increased attention has also raised awareness of the multistakeholder model, including questions about the model's legitimacy and whether this is the right governance structure.

With regard to the Public Comment process, some participants questioned the purpose of Public Comment proceedings and how public comments are taken into account in finalizing policies and recommendations.

- **Summary of Risks Identified During the Trend Sessions**
    - Reduced or insufficient community participation could have an immediate impact on ICANN's ability to do its work (slowing down community's work). It presents risks of capture and poses an existential threat to ICANN's multistakeholder model if we end up with insufficient representation of the various stakeholders.
    - Trust in as well as the credibility and legitimacy of ICANN and its multistakeholder model are at risk.
- **Additional Observations from ICANN Org's Strategic Outlook Network**
    - Several initiatives and other efforts are currently underway that relate to the challenges being raised:
        - In 2019, the Board initiated discussions with the community to develop a work plan towards *Enhancing the Effectiveness of ICANN's Multistakeholder Model.*
        - More discussions about prioritization are happening in the community as well as between the community, organization, and Board. The Board, the community and ICANN org are reviewing priorities.
        - The COVID-19 pandemic response around the world has changed how community participation can be supported through online platforms and how virtual engagement can be delivered to support ICANN's technical and policy work.

        - Lastly, the *Information Transparency Platform* (ITP) will require substantial changes to how Public Comment proceedings are run.

    - Regarding public comments, ICANN published in May 2020 an updated Public Comment Data Analysis Report. The annual report represents an assessment of overall trends in the Public Comment process at ICANN throughout the ten-year period of 2010-2019. The report indicates that the total number of Public Comments proceedings continues to decline by about 7% each year. It underscores a significant increase in participation levels over the last two years (from 5-7 submissions per proceeding between 2010 and 2017 to 9.5 and 8.5 in 2018 and 2019). The overall length of proceedings has been stable throughout the past eight years at 50-52 days.

Financials (and Domain Name Industry) Trends

- **Summary of Trend Elements Collected During the Trend Sessions**

  Within the gTLD marketplace, market consolidation continues and business continuity issues have arisen. In addition, there are community concerns over .COM price cap removals in terms of potential increases in domain registration fees. In addition, there are new investment interests in the domain name industry, including an influx of private equity from "nontraditional" participants. There is increasing unpredictability due to the onset of a global recession, coupled with a greater reliance on the Internet across many sectors. Significant market shifts may affect gTLDs' business continuity and critical functions. Costs of doing business for registries and registrars could increase as a result of fraudulent domains related to COVID-19 as well as to comply with GDPR-related requirements.

  Some participants raised questions about the financial validity of a new round of gTLDs, considering the market's relatively flat growth. In particular, there are low levels of IDN adoption and new gTLD utilization. Although, it is worth noting that some gTLDs have unusually high sales (e.g., .top, .icu). Others anticipated that pressure for a new round of gTLD expansion will increase.

  The combination of market changes could lead to reduced funding for ICANN. These include a perceived lack of interest in new gTLDs, gTLD terminations or revocations, decreasing voluntary contributions from ccTLDs (e.g., .cn, .tw), loss

of Continued Operations Interest (COI) obligations, and more requests for ICANN to waive or defer payment for its fees.

ICANN's running costs are expected to increase in order to implement community policy decisions. For example, implementing the Standardized System for Access/Disclosure (SSAD) that is under development by EPDP Phase 2 is expected to have very high initial costs and liability. There will also be additional costs with future rounds of new gTLDs.

The COVID-19 pandemic is putting financial pressure on all actors in the domain name space, including ICANN. The degree to which COVID-19 measures will affect costs (or yield savings) for meetings, travel, and infrastructure remains unclear. It will be important to consider both immediate and long-term associated effects on the domain name industry and on ICANN's budget. The pandemic may also be accelerating the trend of a national focus and engagement on ccTLDs as critical for disseminating public information. This focus on ccTLDs emerged in 2019 in relation to differences in policies between ccTLDs and gTLDs.

- **Summary of Risks Identified During the Trend Sessions**
    - Marketplace consolidations may have an impact on the competitive landscape.
    - Marketplace shifts combined with a global recession could increase business continuity risks. A global recession could also hasten the rate of TLDs sunsetting and the abandonment of small- and medium-enterprise domains, potentially creating security threats. Global financial conditions also increase the risk associated with Continued Operations Interest (COI) obligations being released without an alternative plan, potentially exposing ICANN to additional Emergency Back-end Operator costs in the event of registry failures.
    - Marketplace and resulting budgetary changes could affect ICANN org's ability to respond to community policy decisions (e.g., Standardized System for Access/Disclosure (SSAD), subsequent procedures), ultimately leading to a loss of trust in ICANN.
    - Funding models based solely on numbers of registrations may not be sustainable in a recession if registrations and renewals continue on a downward trend.

- Changes in the domain industry could create a sense that Registry Operators do not believe in the new gTLD program.
- The global economic downturn caused by COVID-19 will amplify financial trends and the risks associated with them.
- Decreasing funds and increasing costs could lead to future potential deficits for ICANN.

- **Additional Observations from ICANN Org's Strategic Outlook Network**

  There is a misperception that ICANN has control over market changes such as TLD performance, failure rates, domain squatting, and gTLD ownership.

  There is also a broader misperception that ICANN sets policies for ccTLDs and therefore when problems arise, ICANN is responsible.

  The funding forecast that ICANN uses in its budget and 5-year plan leverages historical data, inputs from contracted parties, industry trends, etc., in the process. One challenge is that ICANN org projects far in advance, over a year out, which creates some issues. However, revisions can be made on the basis of public comments received on draft projections and forecast updates before Board adoption. For example, this year the projections were revised to account for COVID-19 impact.

Appendix C | Operational Excellence Trends Assessment

Org's Operational Excellence Trends

- **Statistical Analysis**

The below table identifies, for the trend elements collected during the trend sessions, the number of times a topic was voted top priority, and the number of trend statements collected relating to that topic.

Topics	Priority Votes	Total Trend Statements
Org Internal Efficiencies	24	23
Internal Systems & Tools Challenges	19	20
Talent Acquisition & Retention	19	17
Decision Making Process / Delegation of Authority	11	2
External Demands / Demands for Community Support	7	5
Workload and Pressure on Staff	6	10
Globalization (of ICANN)	4	4
COVID-19	3	4
Succession Planning	2	2
Staff Training & Skills	1	7

The topics of *Org Internal Efficiencies* and *Internal Systems & Tools Challenges* predominated in 2020, both in numbers of votes and number of statements, followed by the topic of *Talent Acquisition & Retention.*

Refer to the Trend Sessions Data Recap spreadsheet to view the detailed statements collected by topic.

This focus area was introduced in the framework for the first time this year. No data is available at this time for year-on-year comparison.

- **Summary of Trend Elements Collected During the Trend Sessions**

  ICANN org faces operational inefficiencies. Some examples cited include:

  - Little follow-up or clarity on new initiatives leading to inefficiency and duplication of efforts.
  - Persisting inconsistencies in end-to-end processes and roles across departments
  - Lack of a communications strategy leading to disjointed messaging and overwhelming amounts of impenetrable content.
  - Lack of cross-functional collaboration, although this trend seems to be improving, particularly in some regions (e.g., APAC).
  - Functions still operating in silos and regional offices not being consulted as SMEs. Lack of regional SMEs in some functions (e.g., Legal, Policy)

  Decision-making is recentralizing at the executive level and in Los Angeles. This is slowing down processes, with increasing levels of bureaucracy involved. This lack of empowerment (among staff and regional offices) is causing inefficiencies and inability to move forward with certain decisions. Recentralization is also causing remote staff to feel left aside.

  Evolving ICANN's systems and tools continues to present challenges. Statements on this include:

  - Lack of a centralized system leads to piecemeal/duplicative processes.
  - There are too many systems being launched simultaneously (e.g., HR). This trend is improving but there are still many systems initiated concurrently.
  - End users are insufficiently involved in design and testing phases of systems, resulting in poor system implementation (e.g., Oracle, Salesforce/ICANN CRM).
  - There are increasing issues relating to the maintenance and the consistency of data sets across ICANN multiple systems and applications.

As it relates to human resources, while recruitment continues to present challenges, the focus is shifting from talent acquisition to concerns of retention and professional development. Observations from participants included:

- Flattening of budget is affecting talent retention due to perceived downgrade in benefits and lessened opportunities for promotion.
- There is a perception of increasing staff turnover, especially among more experienced staff.
- Many new hires and promotions are LA-based which presents a challenge for ICANN's legitimacy as a global organization.
- The process for transferring from one function to another is complex and doesn't favor those moves.

A flat budget combined with increasing demands from the strategic plan puts new stressors on the organization. There are also increasing demands on a core group of SMEs.

It is unclear how ICANN would support a new round of gTLDs with current resources available. Even with current workloads, there is a headcount deficit in some areas.

COVID-19 may impact ICANN operations, meetings, and funding capabilities. The pandemic is creating demand for remote meetings and requiring that staff work remotely, presenting new operational challenges. There is additional uncertainty around regional offices given the travel restrictions and work from home orders due to COVID-19, and uncertainty on phased return to in-person meetings and engagements.

- **Summary of Risks Identified During the Trend Sessions**
  - Organizational and systems inefficiencies affect staff ability to do their work and could lead to wasted time and money.
  - Recentralization of organizational activity in the Los Angeles headquarters (e.g., new hires, centralized processes) is alienating regional and remote staff, decreasing organizational trust, and affecting the credibility of ICANN as a global organization.
  - Slow decision-making and increasing workload on staff may affect ICANN org's timeliness in addressing community expectations.

- Flat budget and increased demands could disrupt operations, decrease organizational agility, and impede our ability to effectively deliver multiple simultaneous projects.
- Multiple factors are contributing to higher risk of decreased team morale and higher turnover (Reduced perspectives of career evolution in an organization that is no longer growing; increasing workloads and pressure on staff; lasting impossibility of meeting face-to-face; poor socio-economic context, etc.)
- Loss of knowledge and institutional memory could result from the departure of experienced staff.

- **Summary of Opportunities & Suggested Actions Identified During the Trend Sessions**

  There are a number of opportunities to take action to address operational excellence trends and associated risks. Ideas include:

  - Foster a more proactive approach by planning and prioritizing incoming work cross-functionally.
  - Improve and harmonize end-to-end processes and roles cross-functionally (e.g. in the case of significant hand-offs between functions) and deepen functions within regional offices. Explore ways to better involve regional offices at earlier stages.
  - Use data to improve operations, inform policy development, and make better informed decisions.
  - Delegate authority and empower regions and non-executive senior management teams to make more decisions at a regional level and outside of the executive team to speed-up processes and reduce bottlenecks.
  - Improve internal communications and general education within ICANN, especially during extended periods of remote working/isolation. Examples include:
    - Increase frequency, volume, and effectiveness of internal communications.

        - Ensure staff is able to carry consistent messaging and understands what is behind those messages.
    - Ensure adequate training is provided for:
        - Onboarding of remote workers.
        - Staff in new roles, as well as when new systems are introduced.
        - Management team leadership skills.
        - Security precautions for all staff.
        - Staff understanding of ICANN's role.
        - Developing technical skills and building Staff capabilities to bridge technology and policy.
    - Communicate more on attrition. Develop succession plans to support smoother transitions to new staff, and increase hiring outside of the US.
    - Leverage functional expertise in remote capabilities (e.g., Policy and MSSI staff have extensive remote experience and best practices that can be shared and utilized by other staff functions).

  Opportunities for improving internal systems and tools include:

    - Ensure effective rollout of the ICANN Customer Relationship Management (CRM)
    - Assess ICANN org staff requirements prior to system planning and involve end users for system testing from initial stages.
    - Automate processes.
    - Expand Salesforce to other parts of the organization.
    - Adopt centralized governance of ICANN data (e.g. consistent documentation of requirements and data models, data dependencies across systems, a centralized country and territory database and other master/referential data, etc.)

- **Additional Observations from ICANN Org's Strategic Outlook Network**

In terms of leadership skills, ICANN's Human Resources function is doing quite a lot (and possibly too much?) with its ICANN LEAD program, but it is not clear that all managers and executives are taking this training. People managers at ICANN, in addition to managing people, also have to be individual contributors, project managers, and subject matter experts in cross functional projects. This leads to not only overworked managers, but little time to just be good people leaders. Adding on mandatory leadership training is not necessarily helping.

This observation leads to a more general trend of the organization jumping to conclusions, pushing out new tools, launching new projects and new programs as remedies to issues that have been identified, without analyzing the reasons for the issues and exploring adequate solutions. (For example, is leadership training efficiently addressing motivation and team morale issues?). It would also be beneficial, post-implementation of new tools or new programs, to determine if they have been effective.

A quick win in relation to the LEAD program would be to make better use of our new training tool, ICANN University, by putting required sessions into smaller blocks rather than three hour sessions, so that managers can follow at their own pace while dealing with increased virtual sessions, webinars, and calls during current work from home situation.

A *Project Management Network* was formed in 2020 as one of the CEO's FY20 goals to identify, develop, and adopt a set of consistent, repeatable project management standards to use across the organization.

In March 2020, ICANN officially launched version 1.0 of the Open Data Platform. The platform provides easier access to ICANN data.

- **Trends Evolution**

Previous Years' Trends:

- [2.3 *(from 2017 - was merged with 2.1 in 2018)*] Increasing operational performance challenges of ICANN organization as it grows in size and complexity.

- [3.3 (from 2017 - was merged with 2.1 in 2018)] Increasing pressure to further globalize impacting distribution of resources.

Shifts in Trends:

- While in recent years operating challenges were mostly due to the increasing size of the organization and the community, these challenges are now more linked to an increasing workload and complexity of work for both organization and community.
- Regarding human resources, the focus is shifting from talent acquisition to concerns of retention and professional development.

- The COVID-19 pandemic is exacerbating a trend which originated with the flattening of the budget, in exploring how to enhance team morale, motivation, and retain talents.
- Recentralization of organizational activity in LA headquarters.

2020 Trends Proposal

- [2.3 *revived and adjusted from 2017*] Operational performance challenges are increasing as ICANN's budget flattens and organization and community workloads grow in size and complexity.

- [2.4 *new*] In a competitive global job market, ICANN continues to face challenges in attracting and retaining talent

- [3.3 *revived and adjusted from 2017*] Inefficiency and centralization of decision making processes at the headquarters - in a context of increasing localized needs as the community diversifies - is slowing down processes and limiting ability to move forward, particularly affecting regions and remote staff.

Appendix D | Trend Impact Assessment Framework

The impact assessment framework used for the trends is available in the separately attached Excel document entitled “2020 Trend Impact Assessment Framework.xlsx”

Appendix E | Background Context

The strategic outlook trend identification is an annual process, which ensures ICANN has a consistent way to:

- Identify and track trends.
- Prepare for opportunities.
- Mitigate or avoid challenges.
- Inform strategic and operational planning and prioritization.

It is a joint effort between the organization, the community, and the ICANN Board to engage on emerging or evolving trends that affect ICANN. Trends indicate general directions in which things are developing or changing, that have or could have an impact on ICANN, its mission, its operations, or its ecosystem. Trends can be internal or external, organization-specific, community-related, or go beyond ICANN's ecosystem as ICANN does not operate in a vacuum.

The organization has found the exercise to be beneficial to help surface opportunities and challenges that lay ahead, inform planning, help with prioritization considerations, and risk management.

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

instagram.com/icannorg

Pages 84-106 Removed - Privileged & Confidential

ICANN BOARD SUBMISSION NO. 2020.12.17.2b

TITLE: **ICANN Organization Risk Appetite Statement**

PROPOSED ACTION: **For Board Consideration and Approval**

EXECUTIVE SUMMARY:

The Board is being asked to consider and adopt the ICANN Organization Risk Appetite Statement (Risk Appetite Statement). The Risk Appetite Statement: (i) articulates the level of risk which ICANN organization is willing to take and retain on a broad level to deliver its mission; (ii) fulfils the Risk Management Framework target model as set by the Board; and (iii) informs the operations of ICANN organization.

BOARD RISK COMMITTEE (BRC) RECOMMENDATION

The BRC recommends that the Board adopt the proposed ICANN Organization Risk Appetite Statement.

PROPOSED RESOLUTION:

Whereas, the ICANN Board previously recognized the benefit of and need for a Risk Management Framework to guide the ICANN organization in managing risks it faces.

Whereas, the ICANN Board previously set a target model for the Risk Management Framework including a Risk Appetite Statement.

Whereas, risk management involves the identification of vulnerabilities to the organization and therefore it would not be prudent to publish the Risk Appetite Statement.

Resolved (2020.12.17.xx), the Board approves the ICANN Organization Risk Appetite Statement and directs the President and CEO, or his designee(s), to publish a summary of it.

PROPOSED RATIONALE:

This Risk Appetite Statement articulates the level of risk which ICANN organization is willing to take and retain on a broad level to deliver its mission.

The ICANN Organization Risk Appetite Statement:

- Communicates to personnel that they need to pursue objectives within acceptable risk limits.
- Provides input for prioritization for planning and budgeting.
- Guides the Board and in its decision making and can be considered as part of the rationale that accompanies Board resolutions.
- Informs performance management and incentive measurement, and guides personnel to make decisions that are aligned to the organizational risk appetite.
- Encourages a risk management, not risk aversion, culture so that risk management is a responsibility shared across the organization and for which all personnel are accountable.
- Enhances ICANN's reputation by demonstrating that the organization is committed to proactively managing risk.

The ICANN Board and the ICANN Executive Team require that a robust Risk Management Framework be developed and implemented for ICANN organization. As part of the Target Operating Model for Risk Management, a Risk Appetite Statement is part of a mature framework.

The Board of Directors and the ICANN org is Executive Team responsible for making informed decisions to set the level of accepted risk. The Risk Appetite Statement specifies the risks the organization is willing to take and retain, thereby demonstrating the risk appetite of the leadership of ICANN which can then be used to guide the operations of ICANN.

Note that by design any Risk Appetite Statement is a high-level articulation of the risks faced by an organization. The intention is to provide a concise overview that is accessible to all personnel and the Board. Further, risks often involve vulnerabilities or threats to the organization, and it would be imprudent for any organization to provide public details of such risks.

The Risk Appetite Statement was developed by the organization's Risk Management function in collaboration with representation of every organization function. The Risk Appetite Statement was reviewed by the organization Executive Team and approved by the ICANN President and CEO for consideration by the Board Risk Committee. The Board Risk Committee reviewed and recommended that the Board approve the ICANN

organization Risk Appetite Statement. The Board received a presentation on the Risk Appetite Statement earlier in 2020.

Adopting the Risk Appetite Statement is in the public interest and is also fully consistent with ICANN's mission as it articulates the risk appetite of the leadership of ICANN which can then be used to guide the operations of ICANN organization more efficiently and consistently from a risk management perspective.

Adopting the BRC's recommendation has no financial impact on ICANN that was not otherwise anticipated; and it formalizes the Risk Management Framework of ICANN organization, and strengthens its approach to managing the risks it faces, therefore could have a positive impact on the security, stability and resiliency of the domain name system.

This is an Organizational Administrative Function that does not require Public Comment.

Please see the Reference Materials Document

Submitted By:	James Caulfield
Date:	12 November, 2020
Email:	james.caulfield@icann.org

Pages 110-131 Removed - Privileged & Confidential